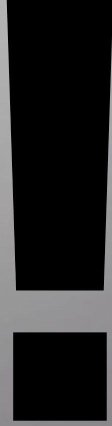
BİLGİGÜVENLİĞİ DERNEĞİ DESTEĞİ İLE YAYIMLANMAKTADIR

Sayı 24
Ocak 2018
20 TL
ISSN 2458-8229
9 772458 822008

CyberMag

TÜRKİYE'NİN İLK VE TEK **SİBER GÜVENLİK DERGİSİ**

CyberMag 3 YAŞINDA





Zaman Daralıyor

Kişisel Verilerin Korunması Kanunu'nun **Uygulama Süreci ve Gereklilikleri**



Kişisel Verileri Koruma Kurumu Başkanı

Prof. Dr. Faruk Bilir İle Söyleşi

Kişisel Veri Dostu Sistemler İçin **Tasarımda Veri Koruma Prensipleri**

Türkiye'de İnternet Dolandırıcılığının Maliyeti **%47 Arttı**



SİBER GÜVENLİK
DEĞERLENDİRME TEST LABORATUVARI





KALİTE VE GÜVENLİK DEĞERLENDİRME

- Ortak Kriterler
- Temel Seviye Güvenlik Değerlendirmesi



GÜVENLİK VE TEST SERVİSLERİ

- Kaynak Kod Analizi
- Sızma Testi
- Kalite Güvence ve Test Otomasyon Servisleri
- Kullanıcı Arayüz Testleri



EĞİTİM VE DANIŞMANLIK

- Ortak Kriterler
- ISO/IEC 27001
- Güvenli Yazılım Geliştirme



ORTAK KRİTERLER

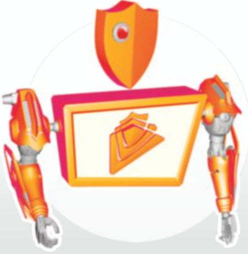
www.BEAMTEKNOLOJİ.com



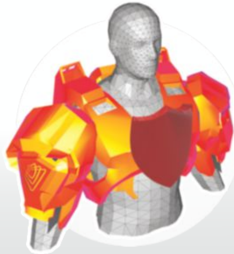
atarlabs

Siber Saldırılar Otomatik, Ya Savunmanız?

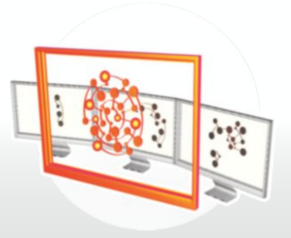




ATAR®'la Siber Alarmları Otomatik Yanıtlayın



Analist Verimliliğini Arttırın



SOC Performansınızı Ölçün ve Raporlayın

Güvenlik Orkestrasını ATAR®'la Yönetin!

www.atarlabs.io

ATARLABS BİLİŞİM A.Ş. Ankara Teknolojileri Gel. Bölgesi Üniversiteler Mh. 1605. Cd. No:3/A Cyberpark E Blok 2. Kat No: 212 Bilkent, ANKARA

www.atarlabs.io | atar_labs | atar-labs | info@atarlabs.io



CyberMag
TÜRKİYE'NİN İLK VE TEK
SİBER GÜVENLİK DERGİSİ

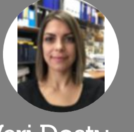
İÇİNDEKİLER

6 Söyleşi

Prof. Dr. Faruk Bilir ile Söyleşi
Kişisel Verileri Koruma Kurumu Başkanı

12 Makale

ZAMAN DARALIYOR!
Platin Bilişim
Kıdemli Sistem Mühendisi
Cemile DENEREL BAŞAK

14 Makale

Kişisel Veri Dostu Sistemler İçin Tasarımda Veri Koruma Prensipleri
Araştırma Görevlisi, Szeged Üniversitesi, Siyasal Bilimler ve Hukuk Fakültesi
Gizem Gültekin Várkonyi

16 Söyleşi

Rahmi Aktepe ile Söyleşi
Türkiye Bilişim Derneği Genel Başkanı

24 Haber


2018 Yılına Damgasını Vuracak Siber Güvenlik Trendleri

26 Haber


Siber Zorba Olma

29 Haber

2018'de Hazırlıklı Olunması Gereken 5 Bulut Bilişim Trendi

30 Haber


Türkiye'de İnternet Dolandırıcılığının Maliyeti %47 Arttı

31 Haber


Fidye Saldırılarının Yüzde 26'sı Şirketleri Hedef Alıyor

32 Haber


Bitcoin Değer Kazandıkça, Kesintiler Daha Çok Can Yakıyor

34 Haber


Tech Data FutureIT Etkinliği Sektörü Buluşturdu

36 Haber

Yaklaşan Tehlike Siber Zorbalık

37 Haber

3. Uluslararası Siber Savaş ve Güvenlik Konferansı Gerçekleştirildi

38 Haber

SHIELD 2017 Konferansı Gerçekleştirildi

40 Haber

NETAŞ ve ZTE'den Türkiye'de Ar-Ge Atağı

Yerel Süreli Yayın
Ocak 2018 / Sayı: 24
Tahsis Edilen ISSN:2458-8229
www.cybermagonline.com

Genel Yayın Yönetmeni
Abdulkerim Oğuzhan Alkan
0532 428 38 38
oalkan@cybermagonline.com

Editör
Prof. Dr. Şeref Sağıroğlu

Danışma Kurulu
Prof. Dr. Mustafa Alkan
Prof. Dr. Ertuğrul Karaçuha
Ahmet Hamdi Atalay
Taha Yücel
Alparslan Bayraktar
Ensar Kılıç
Cengiz Doğan
Kamil Orman
Muhterem İlhan
Burhanettin Al
Murat Dörterler
Alper Doğru

Hukuk Danışmanı
Prof. Dr. Murat Atalı
Fatih Erdöl

Haber Merkezi
Burak Tatar

Görsel Yayın Yönetmeni
Yeşim Önal

Sorumlu Yazı İşleri Müdürü
Abdulkerim Oğuzhan Alkan
0553 008 38 38
oalkan@cybermagonline.com

Reklam Koordinatörü
Ozan Kazancıoğlu
0531 924 35 92
ozan@cybermagonline.com

Web Koordinatörü
Onur Asiliskender
Alkabi Basın Yayın
Danışmanlık ve Organizasyon A.Ş. adına sahibi
Abdulkerim Oğuzhan Alkan
Şenlik Mah. Beyler Sok. 3/12 Keçiören Ankara
0312 381 66 29
info@cybermagonline.com

Matbaa
DUMAT Ofset Matbaacılık San. Tic. A.Ş.
Bahçekapı Mah., 2477 Sokak No:6, Şaşmaz
Etimesgut / Ankara

Sosyal Medya
https://twitter.com/CyberMag_
https://www.linkedin.com/groups/8361527/profile

CyberMag, Türkiye Cumhuriyeti yasalarına göre ALKABİ Basın Yayın Danışmanlık ve Organizasyon A.Ş. tarafından yayımlanmıştır. CyberMag'in isim ve yayın hakları ALKABİ Basın Yayın Danışmanlık ve Organizasyon A.Ş.'ye aittir. Bütün hakları saklıdır. Referans ve alıntı kaynak doğru bir şekilde gösterildiği sürece yapılabilir. Reklamların sorumluluğu yayımlayan firmalara, makalelerin sorumluluğu yazarlarına aittir. Reklam ve makaleler ALKABİ Basın Yayın Danışmanlık ve Organizasyon A.Ş. veya CyberMag'in görüşlerini yansıtmayabilir.



YENİ BİR YILA BAŞLARKEN…

Dünyada bilgi güvenliği ve siber güvenlik alanında yaşananları değerlendirdiğimizde, siber tehditlerin, saldırıların ve suçların arttığını, bunların etkilerinin büyüdüğünü, pek çok kişi, kurum ve devletin bundan olumsuz etkilendiğini, siber güvenlik etki alanının genişlediğini, şirketlerin, kurumların ve ülkelerin konuya olan ilgilerinin arttığını görüyoruz.

Siber güvenlik, artık hayatımızın bir parçasıdır ve gittikçe daha fazla önem verilmesi gerekmektedir. İnternete bağlı olan kullanıcılar için güvenlik veya savunma ortak bir sorun olup, ona bağlı olan her cihaz, sistem, bilgisayar veya sunucu da bunun bir parçasıdır.

2017 yılına baktığımızda bizleri meşgul eden önemli olayların başında, WannaCry, NotPetya gibi fidye yazılımları gelmektedir. Mayıs'ta çıkan WannaCry, 250.000'den fazla sistemi ve 150'nin üzerinde ülkeyi etkilemiştir. Bundan bir ay sonra çıkan NotPetya fidye yazılımı ülkelere daha fazla zarar vermiştir. Verdiği zararın mali boyutu ise yüksektir. Önemi ise, saldırılardan veya zafiyetlerden kolay para kazanma yolunu açmıştır. Diğer önemli bir husus ise mahremiyet ihlalleridir. River City Media'dan 1,37 milyar e-posta sızdırılmıştır. 10 Milyon akademisyenin e-postası ve şifreleri internettedir. Equifax, 143 milyon ABD vatandaşının kimlik ve kredi bilgilerini koruyamamıştır. Über, müşteri, şoför ve araç verilerinin çalınmasını örtbas etmeye çalışmıştır. Facebook, mahremiyeti ihlal ettiği gerekçesiyle Fransa ve İspanya (AEFD) Kişisel Verileri Koruma Kurumları tarafından 1,550 milyon dolar para cezasına çarptırılmıştır. Ülkemizin seçmen kimlik bilgileri internette paylaşılmıştır. Bunların sayısını artırmak mümkündür. Siber savunma için yeni teknik ve teknolojiler, metotlar, yöntemler ve çözümler geliştirilse de mahremiyet ihlallerinde artışlar beklenmektedir. Yeni yılda, dünyada mahremiyet ihlallerinin sayısında büyük artışlar beklenmektedir.

Ülkemizde kişisel verilerin korunması konusunda farkındalık artmaya başlamıştır. Artık, bu alan düzenlenmiştir. Bir kanunumuz vardır. Kişilerin ve kurumların bunlara dikkat etmesi gereklidir. Cezalar caydırıcıdır. Burada unutulmaması gereken husus ise, ülkemizde kanun maddelerini bahane ederek Ar-Ge çalışmalarının engellenmemesidir. Yeni akademik ve sektörel çalışmalarının yapılabilmesi, yeni ürün, fikir, proje ve teorilerin geliştirilebilmesi için verilerden faydalanılmalı, kanunda getirilen Ar-Ge istisnası göz önüne alınarak çalışmalar yürütülmelidir. Kişisel gözlemim, bu konunun iyi anlaşılamadığıdır. Yeni yılda bu konulara açıklık getirilmesi faydalı olacaktır. Bunun için bu sayımızda Kişisel Verileri Koruma Kanunumuz ele alınmıştır. 6698 Sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 yayımlanmış, kurullar oluşturulmuş ve Ocak 2017'de ise bu kurul çalışmaya başlamıştır. KVKK Başkanı Sn. Prof. Dr. Faruk BİLİR'in bu kurulun yapılanması ve kanunla ilgili görüşlerine bu sayıda yer verilmiştir.

Sonuç olarak; dijitalleşen dünya, hayatımızı kolaylaştırsa da yeni fırsatları ve maalesef tehditleri de beraberinde getirmektedir. Kullanıcıların, kişisel verilerini koruyabilmeleri için daha fazla bilgi birikimine, yeteneğine ve yüksek farkındalığa sahip olmalarına gerek vardır. Bunu yapmak zor olsa da mutlaka çaba sarf edilmesi ve konuya daha fazla önem verilmesi gerekmektedir. Kullanıcıların, güvenliği daha basit öğrenebilmeleri, uygulamaları ve kolayca yönetebilmeleri için kurum ve kuruluşların hızlı çözümler geliştirmeleri kaçınılmazdır.

Geleceğimizin daha iyi, mutlu, başarılı ve güvenli olması için, yeni bir yıla geçişi bir fırsat olarak görüp, kişisel, kurumsal ve ulusal bilgi güvenliğimizi gözden geçirmeli, eksikliklerin ve aksaklıkların giderilmesi, sorumluluklarımızın farkında olunmalı, tehditlerin daha yakın takip edilmesi ve en önlemlisi ise yeni nesil tehditlere karşı ortak çözümler geliştirilmeli, karşılaşılan veya karşılaşılabilecek olumsuzlukların yaşanmaması için "siber güvenlik yaşam döngümüzü" oluşturmalıyız.

Mutlu, sağlıklı, huzurlu, güvenli ve özellikle güven dolu bir yıl diliyorum…

Prof. Dr. Şeref SAĞIROĞLU
Editör



Kişisel Verileri Koruma Kurumu Başkanı Prof. Dr. Faruk Bilir ile söyleşi

Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide sektörleri yönlendirerek özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak ve toplumun ilgili tüm kesimleri tarafından ulaşılabilen ve ihtiyaçları önceden karşılayabilen bir kurum olarak kişisel verilerin korunması ile buna ilişkin vatandaşlık bilincinin oluşmasında etkin ve uluslararası alanda söz sahibi bir otorite olmak gayesiyle çalışmalarını yürüten Kişisel Verileri Koruma Kurumu Başkanı Prof. Dr. Faruk Bilir ile; siber güvenlik alanında bilgi ve bilinç düzeyini arttırmak, konu ile ilgili teknolojik gelişmeleri izlemek, milli teknolojilerin geliştirilmesine katkı sağlamak, bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak amacı ile Türkiye'de bilişim sektörünün durumu, devletimizin kalkınmasında BT ve Telekomünikasyon sektörünün yeri ve bilhassa siber güvenlik ve Kişisel Verilerin Korunması Kanunu kapsamında bilinmesi gerekenler ve çözüm önerileri konularında ülkemizin bugünü ve geleceği adına yapılması gerekenleri konuştuk.

CyberMag: Öncelikle Kişisel Verileri Koruma Kurumu'nun kuruluş sürecini anlatır mısınız?

Prof. Dr. Faruk Bilir: 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete-de yayımlanarak yürürlüğe girmesini takiben Kurul üyeliği için seçimler tamamlanmış, Kurul üyeleri 12.01.2017 tarihinde Yargıtay Birinci Başkanlık Kurulu huzurunda yemin etmişler ve üye olarak seçilenler arasından yapılan oylama ile başkan ve ikinci başkan seçilmiştir. Kurum, idari - mali özerkliğe sahip ve kamu tüzel kişiliğini haiz olup Kişisel Verileri Koruma Kurulu ve Başkanlık teşkilatından oluşmaktadır.

CyberMag: Kurumunuz bünyesinde yapmış olduğunuz çalışmalar neticesinde Kurumun nihai amaç ve hedefleri nelerdir?

Prof. Dr. Faruk Bilir: Özel hayatın gizliliğini koruma, temel hak ve özgürlüklere saygı, tarafsızlık, bağımsızlık, güvenilirlik, hukuka ve etik ilkelere uygunluk, şeffaflık, hesap verilebilirlik, hızlı, doğru ve objektif karar alma, işbirliği ve katılımcılık, ulusal ve uluslararası düzeyde hizmet verme değerleri doğrultusunda Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunmasını teminen; ülkemizde kişisel verilerin korunmasını sağlamak, buna yönelik farkındalık oluşturmak, veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak temel amaç ve değerlerimizdir.

CyberMag: KVKK olarak gerek üniversitelerde gerek kamu ve özel sektör bünyesinde çalıştay, konferans ve seminerler düzenlemektesiniz. Bu çalışmalardan beklentileriniz nelerdir? Umduğunuz verimi alabiliyor musunuz?

Prof. Dr. Faruk Bilir: Kurum olarak çalışmalarımıza başladığımız günden bu yana önceliğimiz kanunu, kanunun hukuk sistemimize katkıları ile kişilere getirdiği hak ve yükümlülükleri ve bu alanda ülkemizin yetkili otoritesi olarak kurumu tanıtmak oldu. Nitekim daha önce kişisel verilerin korunmasına yönelik çeşitli mevzuat düzenlemeleri bulunmakla birlikte, ülkemizde ilk kez 6698 sayılı kanun ile bu alanda başlı başına bir kanuni düzenleme yapılmış ve yetkili bir otorite tesis edilmiştir.



Diğer yandan, alanın güncel ve dinamik bir yapıya sahip olması, teknolojik gelişmelerden çok hızlı etkilenmesi, uluslararası mevzuatın da bir taraftan sürekli değişmesi, bu alanda faaliyet gösterenlerin ve onların faaliyetlerinden etkilenenlerin ihtiyaçlarının da bu etkenlere bağlı olarak farklılaşması, hem konuya ilişkin daha fazla çalışma yapılmasını, hem karşılıklı bilgi alışverişini güncel tutmayı hem de kurum olarak sahadaki son gelişmeleri takip etmeyi gerektirmektedir. Bu bakımdan kurum olarak gerek kamu sektörü ile gerek özel sektör ile işbirliği halinde gerçekleştirilen çalışmaların her anlamda faydalı ve geliştirici olduğunu düşünüyoruz.

CyberMag: Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmelik Taslağı kamuoyunun görüş ve önerilerine sunuldu. Beklediğiniz geri dönüşleri alabildiniz mi?

Prof. Dr. Faruk Bilir: Bugüne kadar hazırlanan yönetmelik taslaklarından hem Veri Sorumluları Sicili Hakkında Yönetmelik hem de Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik kamuoyunun görüş ve önerilerine sunuldu. Her iki yönetmelik taslağına ilişkin olarak gerek özel sektör gerek kamu kurum ve kuruluşları oldukça yoğun ilgi gösterdiler, bu anlamda çok sayıda kuruluş söz konusu düzenleme taslakları ile ilgili olarak görüş ve önerilerini bizimle paylaştı. Bu görüş ve öneriler kurulumuz tarafından değerlendirildi. Bu kapsamda gerekli görülen değişiklikler de yapılarak söz konusu yönetmelik taslakları yayımlanmak üzere Başbakanlığa gönderildi. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik" 01.01.2018 tarihinde yürürlüğe girmek üzere 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlandı.

CyberMag: Kişisel Verilerin Korunması Kanunu'nun 16. maddesinde "Veri Sorumluları Sicili" tutulması hükme bağlanmıştır. Kişisel verileri işleyen gerçek ve tüzel kişilerin kayıt altında tutulmasını şart koşan bu maddenin gerekliliklerini okuyucularımızla paylaşır mısınız? Söz konusu maddeye göre, bazı durumlarda Kişisel Verileri Koruma kurumu, Kurul kararıyla sicile kayıt zorunluluğuna istisna getirilebiliyor. Bu istisnai durumlardan bahsedebilir misiniz?

Prof. Dr. Faruk Bilir: Veri Sorumluları Sicili, veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir. Kişisel veri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Sicile kayıt olma yükümlülüğü, kişisel verilerin işlenmesi faaliyetlerinde şeffaflık

"Özel hayatın gizliliğini koruma, temel hak ve özgürlüklere saygı, tarafsızlık, bağımsızlık, güvenilirlik, hukuka ve etik ilkelere uygunluk, şeffaflık, hesap verilebilirlik, hızlı, doğru ve objektif karar alma, işbirliği ve katılımcılık, ulusal ve uluslararası düzeyde hizmet verme değerleri doğrultusunda Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunmasını teminen; ülkemizde kişisel verilerin korunmasını sağlamak, buna yönelik farkındalık oluşturmak, veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak temel amaç ve değerlerimizdir."



sağlanması ve veri sorumlularının mevzuata uyumlu hareket etmeleri konusunda daha güvenli bir ortam oluşturulması amacını taşımaktadır. Sicile açıklanacak bilgiler; veri güvenliği, süreç optimizasyonu, ekonomik fizibilite gibi oldukça detaylı ve disiplinler arası bir çalışma sonucunda derlenecek bilgilerdir. Veri sorumluları sicilinde hiçbir şekilde gerçek kişilere ilişkin kişisel veriler yer almayacaktır.

İşlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, kurul tarafından, sicile kayıt zorunluluğuna istisna getirilebilir.

Burada öngörülen yalnızca sicile kayıt yükümlülüğünün istisnası olup kişisel verilerin korunmasına ilişkin genel esaslara ve kanunla getirilen diğer düzenlemelere uygun davranma yükümlülüğü devam edecektir.

CyberMag: Oluşturulan Kişisel Verileri Koruma Kurumu hakkında okuyucularımıza bilgi verebilir misiniz? Kurumun nasıl bir yapısı olacaktır? Kurulun ne gibi görev ve yetkileri vardır?

Prof. Dr. Faruk Bilir: Kanunun yürürlüğe girmesi ile birlikte, kanunla verilen görevleri yerine getirmek üzere Kişisel Verileri Koruma Kurumu kurulmuştur. Kurul üyelerimizin seçilmesi ve yemin etmeleri ile birlikte kurum da fiili olarak faaliyetlerine başlamıştır. Kurum, idari ve mali özerkliğe sahip, kamu tüzel kişiliğini haiz ve Başbakanlıkla ilişkilidir.

Kurum; Kurul ve Başkanlıktan oluşur. Kurumun karar organı Kurul'dur.

Kurul, bu kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. Kurul; beşi Türkiye Büyük Millet Meclisi, ikisi Cumhurbaşkanı, ikisi Bakanlar Kurulu tarafından seçilen dokuz üyeden oluşur.

Kurul'un başlıca görevleri; kişisel verilerin temel hak ve özgürlüklere uygun olarak işlenmesini sağlamak, özel nitelikli kişisel verilerin işlenmesinde gerekli ve yeterli önlemleri almak, kişisel verilerin yurt dışına aktarımında yeterli korumanın bulunduğu ülkeleri tespit ve ilan etmek, kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda veri aktarımına izin verilip verilmeyeceğini değerlendirmek, yurt dışına aktarımda uyulacak usul ve esasları belirlemek, veri sorumluları tarafından kuruma yapılan bildirimleri incelemek, ilgili kişi başvurularını incelemek, ilke kararları almak, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâllerinde veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar vermek, sicilin gözetimini yapmak, sicile kayıt zorunluluğuna istisnalar getirmek, düzen-



leyici işlemler yapmak ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek olarak sıralanabilir.

CyberMag: Öncelikle kanunun koruma altına aldığı kişisel veri kavramından bahsedebilir misiniz? Hangi bilgiler kişisel veri kapsamına girer?

Prof. Dr. Faruk Bilir: Kimliği belirli ya da belirlenebilir nitelikteki gerçek bir kişiye ilişkin her türlü bilgi kişisel veridir. Kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir. Bu bakımdan tüzel kişilere ait Veriler Kanunu'nun getirdiği korumanın dışında kalmaktadır. Örneğin, bir şirketin ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin bilgiler kişisel veri sayılmayacaktır. Bunun istisnası ise tüzel kişiye ait bilginin bir gerçek kişiyle ilişkilendirilebileceği durumlardır.

Gerçek kişiye ilişkin her türlü bilgi kanunun koruması kapsamındadır. Örneğin gerçek kişinin; adı, soyadı, doğum tarihi ve doğum yeri, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, fotoğraf, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.

Kanunda hangi bilgilerin kişisel veri olarak kabul edileceğine ilişkin sınırlı sayma yoluna gidilmediğinden kapsamının genişletilmesi mümkündür. Önemli olan verinin gerçek kişi ile ilişkilendiriliyor olması ya da gerçek kişiyi tanımlayabilmesidir. Ancak özel nitelikli kişisel veriler Kanunda sayma suretiyle belirtilmiş olup, bu nitelikteki kişisel verilerin genişletilmesi mümkün değildir.

CyberMag: Kanun kapsamında kural olarak kişisel verilerin işlenmesi için ilgili kişinin açık rızası gerekir. Ancak bazı koşullarda kişisel veri sahibinin rızasının alınmasına gerek yok. Kişisel verilerin işlenmesindeki bu istisnai durumlara örnek verebilir misiniz?

Prof. Dr. Faruk Bilir: Açık rıza, belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür irade ile açıklanan rızadır. Başka bir ifade ile ilgili kişinin veri işlenmesine özgürce, konu hakkında yeterli bilgi sahibi olarak ve sadece o işlemle sınırlı kalmak kaydıyla verdiği onay beyanıdır.

Kanun'da kişisel verilerin açık rıza olmaksızın işlenemeyeceği belirtildikten sonra, açık rıza olmaksızın kişisel verilerin işlenebileceği haller de belirtilmiştir. Kanunlarda açıkça öngörülmesi, fiili imkânsızlık (rıza açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması), bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğü yerine getirebilmesi için zorunlu olması, kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması ve (ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla) veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkündür.

CyberMag: Veri İşleyen ve Veri Sorumlusu kavramları çokça karıştırılıyor. Bu kavramları açıklayabilir misiniz?

Prof. Dr. Faruk Bilir: Veri sorumlusu, kişisel verileri işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Bu kişiler, gerçek kişiler olabileceği gibi kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilecektir.

Veri işleyen ise, veri sorumlusu adına ve veri sorumlusunun verdiği yetkiye dayanarak kişisel veri işleyen gerçek veya tüzel kişidir.

Veri sorumlusunun tespiti için; kişisel verilerin işlenmesi ve işlenme amacı, işlenecek kişisel veri türleri, işlenen kişisel verilerin hangi amaçla kullanılacağı, kimlerin kişisel verisinin işleneceği, kişisel verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kimlerle paylaşılacağı, ne kadar süreyle saklanacağı, ilgili kişilerin erişim hakkı ve diğer haklarının uygulanıp uygulanmayacağı gibi hususlarda kimin karar verdiği dikkate alınır. Örneğin, veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına faaliyet gösteren, dışarıdan hizmet alınması suretiyle çağrı merkezi hizmeti veren bir şirket bu faaliyet kapsamında veri işleyen olarak kabul edilecektir.

> **"İşlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, kurul tarafından, sicile kayıt zorunluluğuna istisna getirilebilir."**



> Açık rıza, belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür irade ile açıklanan rızadır. Başka bir ifade ile ilgili kişinin veri işlenmesine özgürce, konu hakkında yeterli bilgi sahibi olarak ve sadece o işlemle sınırlı kalmak kaydıyla verdiği onay beyanıdır.

CyberMag: KVKK olarak, bilgi güvenliği konusunda çalışma yürüten sivil toplum kuruluşlarına, derneklere destek veriyorsunuz. Bu durum göz önünde bulundurulduğunda, sektör üzerinde bir sinerji oluşturmak ve farkındalık oluşturmak adına sivil inisiyatif organlarına düşen görevler nelerdir?

Prof. Dr. Faruk Bilir: 6698 sayılı Kanunun iyi analiz edilerek uygulamada birlik sağlanabilmesi, kanun ile hem kişisel verisi işlenenlerin hem de kişisel veri işleme faaliyetinde bulunanların hak ve menfaatlerinin gözetilerek, iki tarafın da bu denge çerçevesinde çıkarlarının dikkate alınabilmesi için sektörün ve sektörün etkilediği kişi ve kurumların birlikte hareket etmesi faydalı olacaktır.

CyberMag: CyberMag, siber dünyadaki riskler ve siber güvenlik konusuna odaklanmış Türkiye'nin ilk basılı ve elektronik dergisi olarak farkındalığı artırmayı ve insanları bilgilendirmeyi amaç edinmektedir. Bu amaçla yola çıkan ve yayın hayatına bir seneyi aşkın bir süredir devam eden CyberMag hakkında düşünceleriniz nelerdir?

Prof. Dr. Faruk Bilir: Siber güvenlik gibi spesifik bir alanda, konuya ilişkin güncel gelişmelere, makale, haber ve etkinliklere bir arada ulaşma imkanı veren CyberMag sadece dergi değil aynı zamanda bu alanda çalışanlar için faydalı bir kaynak, bir platform değeri taşımaktadır. Hem firmaların hem de ilgili kimselerin tüm siber güvenlik alanındaki gelişmeleri takip edebileceği ve paylaşabileceği ortak bir nokta yaratılmasının gerekli ve faydalı olduğu açıktır.

CyberMag: Eklemek istediğiniz başka bir konu var mı?

Prof. Dr. Faruk Bilir: Kişisel verilerin korunmasının önemine binaen, ilgili kişiler nezdinde farkındalık oluşturulması amacıyla bugüne kadar kanunun uygulanmasına ilişkin rehber, broşür, soru-cevap kitapçığı çalışmaları gerçekleştirdik, kamu kurum ve kuruluşlarına ve özel sektörde faaliyet gösteren kuruluşlara yönelik çalıştaylar düzenledik. Bu anlamda hazırlanan ikincil düzenlemelere, duyurulara, haberlere ve gerçekleştirilen faaliyetlere, kurumumuzun internet sitesi ile Twitter ve Facebook hesaplarında da yer veriyoruz. Bundan sonraki süreçte de kamuoyu nezdinde farkındalık oluşturulmasını teminen tanıtıcı film, broşür ve kamu spotlarının yayımlanması sosyal medyaya ilişkin çalışmaların zenginleştirilmesi en önemli hedeflerimiz arasında. Bu alandaki gelişmeler ile kurumumuz faaliyetlerini söz konusu mecralardan takip edebilirsiniz.

e-safe
make it safer!

KİŞİSEL VERİLERİ KORUMA ZİRVESİ



Tarih: 18 Ocak 2018
Yer: Kişisel Verileri Koruma Kurumu Konferans Salonu, Ankara
Saat: 09:00 - 17:00



Cemile Denerel Başak

Platin Bilişim Kıdemli Sistem Mühendisi



ZAMAN DARALIYOR!

Son tarih: 07/04/2018 Peki biz ne kadar hazırız?

07/04/2016 tarihinde 6698 numaralı Kişisel Verileri Koruma Kanunu resmi gazetede yayınlanarak yürürlüğe girdi. Uyum süreci için verilen 2 yıllık sürenin sonlarına yaklaşmaktayız.

Kişisel Verileri Koruma Kanunu'nun amacı:

- Anayasada öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması
- Kişinin mahremiyet hakkının korunması
- Kişinin bilgi güvenliği hakkının korunması
- Kişisel verilerin işlenmesinin kontrol altına alınması
- Kişisel verileri işleyen tüzel ve gerçek kişilerin yükümlülüklerinin ve uyacakları usul/esasların belirlenmesi

Kısaca Kişisel Verileri Koruma Kanunundaki tanımları gözden geçirelim.

"Kişisel veri":

Kişisel bilgi ve kişisel veri birbirinin yerine kullanılan ifadeler olmasına rağmen, "bilgi" ve "veri" kelimeleri kavramsal olarak farklı anlamlar içeriyor. Avrupa Birliği'nin Veri Koruma Yönergesi, kişisel veriyi "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri" olarak tanımlıyor. Kimliği belirlenebilir kişi ise "doğrudan veya dolaylı olarak özellikle bir kimlik numarasının veya kişinin fiziksel, fizyolojik, akli, ekonomik, kültürel veya sosyal kimliğine ait bir veya birden fazla spesifik faktörün referansına dayanılarak teşhis edilebilir olan kişi" olarak tanımlanıyor.

KVKK'da kişisel veriler genel kişisel veriler ve özel kişisel veriler (diğer adıyla hassas veriler) olmak üzere ikiye ayrılmıştır. Genel kişisel veriler; ad-soyad, TC kimlik no, doğum yeri, doğum tarihi gibi klasik anlamda kişisel verilerimizden oluşmakta iken hassas veriler kanunda "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel tercihi, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak sayılmıştır.

Hassas verilere ilişkin bir diğer düzenlemede Türk Ceza Kanunu'ndaki m.135/2'dir. Burada hassas veriler "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin" verileri olarak sayılmıştır. Bu verilerin hukuka aykırı olarak kaydedilmesi bakımından diğer kişisel verilere göre iki kat daha fazla ceza öngörülmüştür.



"Veri sorumlusu":

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi belirtmektedir. Konusunda uzman avukat önerileri veri sorumlusunun tek bir kişi olmaması bir kurul belirlenmesi gerektiği yönündedir.

Veri sorumlusunun veri güvenliğini sağlamak adına yükümlülükleri:

- Verilerin hukuka aykırı işlenmesini önlemek
- Verilere hukuka aykırı erişilmesini önlemek
- Verilerin muhafazasını sağlamak amacıyla her türlü teknik ve idari tedbiri almak
- Veri envanterini oluşturmak ve de bu bilgileri VERBIS üzerine girmekle sorumludur.

İşlenen veri kanuni olmayan yollarla başkaları tarafından elde edilirse, veri sorumlusu bunu yetkiliye ve KVK Kurulu'na bildirmek zorundadır.

"Verbis":

Veri sorumlularının sicile başvuru ve sicille ilgili diğer işlemlerde kullanacakları; internet üzerinden erişilebilen, başkanlık tarafından oluşturulan ve yönetilen bilişim sistemine verilen isimdir.

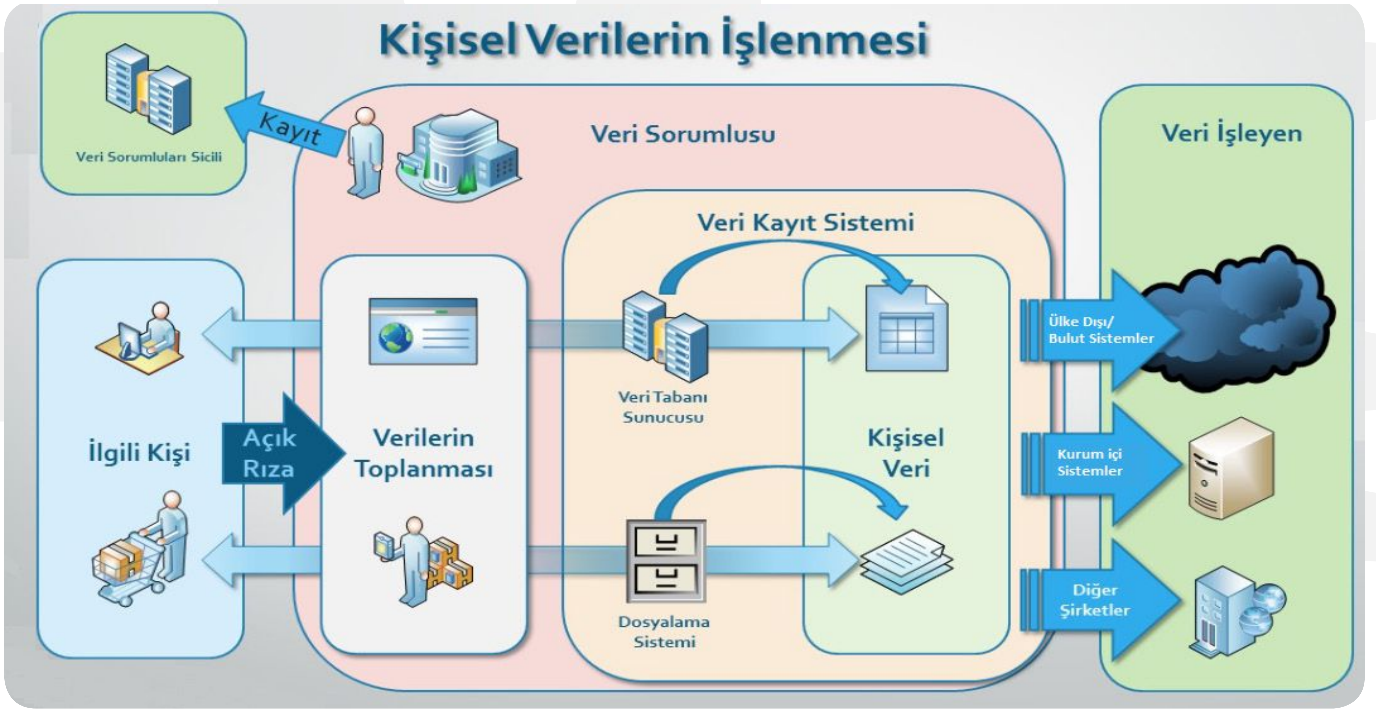
Kişisel verilerden kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde yukarıda belirtilen tedbirlerin alınması hususunda bu kişilerle beraber müşterek olarak sorumludur.

"Veri işleyen":

Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak kanunda geçmektedir.

"Kişisel verilerin işlenmesi":





Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri üzerinden gerçekleştirilen her türlü işlemi içermektedir.

“Kişisel veri işleme envanteri”:



Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve detaylandırdıkları envanterdir.

“Kişisel veri saklama ve imha politikası”:

Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirlemek için dayanak yaptıkları politikadır.

“Anonim hale getirme”:

Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesidir.

Kişisel verilerin kötüye kullanılmasında ve siber suçla mücadelede alınacak tedbirler:

Veri hırsızlıkları, fiziksel ve bilgi işlem güvenliğine yeterince önem verilmemesi, dizüstü bilgisayar hırsızlıkları, korsan faaliyetler, şirket çalışanlarının veri sızdırması gibi farklı şekillerde gerçekleşebilmektedir.

Yasal yaptırımlar:

Yapılması gerekenler:

- Çalışanların eğitilmesi
- Kişisel verilerin işlem süreçlerinin belirlenmesi
- Mevcut IT altyapısının gözden geçirilerek gerekli uygulamaların alınması veya düzenlenmesi
- Hukuki destek

Teknik çözüm önerisi:

En büyük rol bilişim teknolojilerine düşmektedir. Burada düzeni sağlamak için birbiri ile kolay entegre olan ürünler kullanmak ve bunları beraber yönetebilmek büyük önem kazanmaktadır.



Kişisel Verileri Koruma Kanunu yönetilmesi gereken ve sürekli denetlenmesi gerek bir süreçtir. Sürekli kontrol ve denetimlerin yapılması bu noktada çok önemlidir.

Suç Veya Kabahat	*Öngörülen Yaptırım*
Kişisel Verilerin hukuka aykırı olarak kaydedilmesi	*1 - 3 yıl hapis cezası*
Kişisel Verilerin hukuka aykırı olarak verilmesi, yayılması, ele geçirilmesi	*2 - 4 yıl hapis cezası*
Yok edilmesi gereken verilerin yok edilmemesi	*1 - 2 yıl hapis cezası*
İlgili kişiyi aydınlatma yükümlülüğünün yerine getirilmemesi	*5.000₺ - 100.000₺ idari para cezası*
Sicile Kayıt ve Bildirim yapılmaması	*20.000₺ - 1.000.000₺ idari para cezası*
Veri Güvenliği Yükümlüklerine aykırılık	*15.000₺ - 1.000.000₺ idari para cezası*
Kişisel Verileri Koruma Kurulu kararlarına aykırılık	*25.000₺ - 1.000.000₺ idari para cezası*

Kişisel Veri Dostu Sistemler İçin Tasarımda Veri Koruma Prensipleri



Gizem Gültekin Várkonyi

Araştırma Görevlisi,
Szeged Üniversitesi,
Siyasal Bilimler ve Hukuk Fakültesi

Kişisel verilerin korunması hakkı yaklaşık 50 yıldır birçok Avrupa ülkesinin anayasasında yer almakta. Teknoloji geliştikçe, sosyal ağların kullanımı arttıkça, internetten alışveriş yaygınlaştıkça, çevirimiçi sağlık ve finans hizmeti alıcıları arttıkça, her türlü kişisel bilginin çevirimiçi dolaşmaması için çok fazla engel kalmamakta. Firmalar büyük verinin nimetlerinden yasalarla çelişmeden faydalanmanın yollarını aramakta ve bazen gizlilik ile ilgili yasaları engel olarak da görmekte. Ancak aslında çözüm, basit bir adımın zamanında atılmasında saklı.

Tasarımda veri koruma, Kanada'nın Ontario eyaleti Kişisel Bilgi ve Gizlilik Komiseri Ann Cavoukian tarafından 1993 yılında ilk kez bahsedildi. Cavoukian'ın Tasarımda Gizlilik Prensipleri (Privacy by Design) olarak düzenlediği prensiplerin asıl kaynağı, Amerika Birleşik Devletleri Federal Ticaret Komisyonu'nun özellikle 'dijital tüketicilerin' kişisel veri güvenliğini sağlamak adına oluşturduğu ve rehber niteliğindeki Adil Bilgi Uygulamaları prensipleridir. Avrupa Birliği'nin 25 Mayıs 2018'de uygulamaya koyacağı Genel Veri Koruma Tüzüğüne (GVKT, Madde 25) de dâhil edilen Tasarımda Veri Koruma (TVK) kavramı, kişisel verileri koruma hukukunu birçok yönden tamamlayıcı yönlendirmeler yapmaktadır.

TVK prensipleri kişisel veri dostu yazılımların oluşturulabilmesi için gerekli kurumsal ve teknik değerlendirmelerin sağlıklı biçimde yapılabilmesi için atıla-

cak ilk ve sürekli adımları temsil eder. Bu adımlar sayesinde sistem kullanıcılarının güveninin kazanılması öncelikli amaçlardandır. İnternet ekonomisinin gitgide büyüdüğü ve hükmünü artırdığı çağımızda, kullanıcının güvenini kazanmak, sürdürülebilir bir marka değeri oluşturmak için önemli bir noktadır. Örneğin Apple kullanıcılarının sadakati belki de firmanın sık sık dile getirdiği kullanıcı gizliliğine verdiği önemden kaynaklanmaktadır. Kullanıcının güveni söz konusu olduğunda, sistem geliştiricilerinin kişisel verilerin korunması hakkının öncelikli olduğu bir kurum kültürü yaratması şarttır. Böyle bir ortamda kişisel verilerin korunması ile ilgili yapılması gerekenler sistemlerin önünde bir engel değil, aksine sistemlerin değerini en az iyi tasarlanmış bir kod kadar artıran bir bileşen olarak görülmelidir. Kişisel verilerin korunması hakkına saygılı firmaların şüphesiz yasalarla uyumlu ürünler ortaya çıkararak "başlarını belaya sokmayacakları" söylenebilir.

TVK prensiplerinin kısa bir analizi, kavramı daha yakından tanımamıza yardımcı olacaktır. Herhangi bir kişisel verinin ifşası veya yasa dışı olarak ele geçirilmesi özellikle günümüz teknolojisi sebebiyle bu verilerin kurtarılmasını imkânsız ve kişi haklarının ihlalini geri çevrilemez hale getirmektedir. Bu sebeple TVK, sistemde veri güvenliği ile ilgili önlemlerin "Koruyucu ve Engelleyici" biçimde sistem tasarımından da önce düşünülmesi gerektiğini önerir. Bu önlemler, tasarlanan sistemde işlenecek kişisel verilerin risk analizi ile sistemde planlanan teknik önlemlerin analizlerinin yapılması sayesinde netleştirilir. Böylelikle veri koruma ile ilgili her türlü somut önlemin sistem mimarisine "Gömülmesi" amaçlanır. Hangi somut önlemlerin alınacağına ise "Kişisel Veri Etki Analizi" ile karar verilebilir. Her ne kadar bu analizin "veri işlemenin kişi haklarının ihlaline yüksek seviyede risk oluşturduğu durumlarda yapılması" (GVKT, Madde 35) öngörülse de, kişisel verilerin işlendiği her sistemde mutlaka belli bir seviyede risk olduğu göz önünde bulundurulmalıdır. Etki analizinin nasıl yapılması gerektiği ile ilgili örneğin İngiltere Veri Koruma Kurumu ile Avrupa Veri Koruma Denetçiliği'nin dokümanlarından veya Fransa Veri Kurumu'nun henüz geliştirdiği ücretsiz "Etki Analizi" yazılımından veya IBM, Facebook gibi teknoloji devlerinin tecrübelerini paylaştıkları dokümanlardan faydalanılabilir. Etki analizinden sonra firmanın elinde sistemin kişisel verileri koruma yeterliliği ile ilgili somut bir değerlendirme olması beklenir. Bu değerlendirme sonuçlarına göre sistemle ilgili teknik ve kurumsal hangi güçlendirmelerin yapılacağına karar verilmelidir. Teknik konularda Gizliliği Artırıcı Teknolojilerden (Privacy Enhancing Technologies) yararlanılabilir. Bu teknolojilerin bilinmesinin "Kişisel Veri Dostu Sistemler" oluşturmak adına iyi bir başlangıç olacağı söylenebilir. Veri minimizasyonu, sunucu güvenliği, anonimleştirme, depolama gizliliği, yetkilendirme gibi tekniklerden uygun olanların seçilmesi, uygulanması, geliştirilmesi ve gözden geçirilmesi gerekmektedir. Veri minimizasyonu tekniği gereğince, sistemin fonksiyonlarının yerine getirilmesi "asgari veri" yaklaşımı ile sağlanır. Bu yaklaşım, sistemin çalışabilmesi için gerekli en az verinin toplanması, daha fazlası için ise veri sahibinin rızasının alınmasını öngörür. Bu tekniğin kullanıcılara yansıdığı tarafta ise sistemlerde "Veri Korumanın Varsayılan" sistem ayarı olarak sunumu söz konusudur.

Kişisel veri dostu sistemlerin başarılı biçimde tasarlanması için firmaların kişisel verilerin korunmasıyla ilgili attıkları bütün adımları dokümante ederek "Şeffaf ve Görünür" biçimde paydaşlarına, ilgili kurumlara ve sistem kullanıcılarına sunması gerekir. Tüm bilgilerin anlaşılır ve açık biçimde sunulması çok önemlidir, çünkü bu dokümanlar firmaların kişisel verilerin korunması ile ilgili hukuka uyup uymadıklarını kanıtlayabilecekleri dokümanlardır. Dokümanlarda sistemlerin ne oranda "Kullanıcı Gizliliğine Saygılı" biçimde tasarlandığı görünür olmalıdır. Böyle sistemlerde veri sahiplerine kişisel veri yönetimini kolaylaştırıcı araçlar sunulur. Google, Facebook gibi birçok teknoloji devi, kullanıcılarına açık ve anlaşılır bilgi ve yönlendirmelerle donanmış ve çekici biçimde tasarlanmış kişisel veri yönetim panelleri sunmaktadır. Bunun yanı sıra, unutulma hakkı, çocukların veri koruma hakları, verilerin istendiği zaman başka bir sisteme taşınabilmesi gibi Avrupa Birliği Tüzüğü'nde yerini alan hakların da sağlanması gerekir.

Sistemin sürekli olarak izlenip gerekli durumlarda müdahale edilerek veri güvenliğinin sağlanması, gerektiğinde etki analizinin yapılması, veri yönetiminin veri sahibine bırakılması ve gizlilik sözleşmeleri ile veri sahiplerinin haklarının en yüksek seviyeye getirilmesi için güncellenmesiyle birlikte sistemde "Yaşam Boyu Veri Güvenliği" sağlanır. Böyle bir ürünün ortaya konması sonucunda sistemi oluşturanlar başta olmak üzere tüm paydaşlardan sistem kullanıcılarına kadar herkes Kazan-Kazan durumunda olacaktır. TVK prensiplerinin amacı da işte tam olarak budur.



Türkiye Bilişim Derneği Genel Başkanı **Rahmi AKTEPE** ile Söyleşi



> *"TBD Genel Başkanı Başkanı Rahmi Aktepe ile derneğin kuruluş amacı, çalışma ve projelerini ve bilhassa bu yıl Kalkınma Bakanımız Lütfi Elvan'ın teşrifleri ile gerçekleşen, bilişim kurultayını değerlendirdik…"*

CyberMag: Öncelikle bizlere derneğinizden, kuruluş amacından ve çalışmalarından bahsedebilir misiniz?

Rahmi Aktepe: Türkiye'nin bilişimle tanışmasının neredeyse hemen ardından 1971 yılında, bugün bilişim profesyoneli diyebileceğimiz yarı akademik bir topluluk tarafından büyük bir gelecek vizyonu ile kurulan Türkiye Bilişim Derneği (TBD) bugün artık toplumun her katmanından üye yapısıyla "Bilişim Kültürünü" yaymaya çalışan bir "Sivil Toplum" öncü hareketine dönüşmüştür.

Üye sayısı bugün 12.000'i aşmıştır. 6 şubesi, 22 il temsilciliği ve üniversitelerdeki TBD-Genç örgütlenmesiyle TBD, bilişim sektörünün gelişmesine önemli katkılar vermeye devam etmektedir.

TBD, kamu ve özel sektör, akademisyen ve toplumun her kesiminden etkin kullanıcılardan oluşan üye yapısıyla bilişim sektörünün önde gelen bir derneğidir; diğer bir deyişle "Sizin Derneğinizdir".

Türkiye'nin bilişim toplumu olma yolunda atılacak tüm adımlarında olmak ve bu bilişim toplumu olma yolunda toplumdaki bilincin ülke genelinde artmasını sağlamak en büyük amaçlarımızdandır.

TBD'nin bireysel katılımı esas alan yapısı ve gönüllülük temelindeki çalışma biçimiyle ürettiği raporlar, öneriler ve bağımsız söylemleri günümüzde tüm karar vericiler ve toplumun her kesimi tarafından dikkate alınır duruma gelmiştir. Bu başarıda en önemli etmen üyelerinin yıllardır her koşulda derneğimize gösterdiği ilgi, güven, sağladığı destek ve katkıdır.

Derneğimiz, ülkemizin 2023 vizyonuna yönelik olarak başta bilişim politikaları olmak üzere, bilişim sektörünün temel problemleri ile çözüm önerilerinin, teknolojik gelişmeler ve gelecek öngörülerinin, bilişim teknolojilerine ilişkin çok değerli bilgilendirme, değerlendirme ve tespitlerin yapıldığı birçok etkinlikler düzenlemektedir. Bu kapsamda gerçekleştirdiğimiz etkinliklerimizden bahsetmek isterim.

BİMY'24 (TBD 24. Bilgi İşlem Merkezi Yöneticileri Semineri) 27-30 Nisan 2017 tarihlerinde "Bilişimde Gelişim, Bilişimle Gelişim" ana teması ile RIXOS Premium Kongre Merkezi, Belek Antalya'da gerçekleştirildi.

Kamu, özel sektör ve üniversitelerin üst düzey yöneticileri buluşturuldu. 24.sünü yaptığımız BİMY etkinliğimizde AR-GE, ÜRETİM ve İSTİHDAM üzerine mevcut durum değerlendirmesi yanında geleceğe yönelik öngörüler ele alınarak kamu, özel sektör ve üniversitelerin katılım ve katkılarıyla farkındalık yaratılmaya çalışılarak, ilgili kurum ve kuruluşlara sunulmak üzere sonuç raporları hazırlandı.

19.KAMU-BİB etkinliğini ise 26-29 Ekim 2017'de Bodrum'da geniş katılım ile gerçekleştirildi. Etkinlik öncesinde kamunun güncel teknolojik konuları ile ilgili çalışma grupları oluşturuldu.

Gelin 'Dijital Türkiye' için güçlerimizi birleştirelim" sloganı ile yola çıktığımız; Kamu-BİB toplantımızda yıllardır kamuyu ve özel sektörü buluşturarak, ortak bir sinerji oluşturulmasına katkı sağlamaktayız. Etkinliğimizde hükümetin eylem planında da var olan 'Dijital Türkiye' hedefi için kamunun, özel sektörün ve akade-

> "TBD, kamu ve özel sektör, akademisyen ve toplumun her kesiminden etkin kullanıcılardan oluşan üye yapısıyla bilişim sektörünün önde gelen bir derneğidir; diğer bir deyişle **"Sizin Derneğinizdir".**"





> "Siber güvenlikte en zayıf halkanın ve aynı zamanda da en önemli faktörün insan olduğu bilinciyle; insanları eğitmek, bilinçli ve etik bilişim kullanıcıları haline getirmek amacıyla ilköğretimden başlayarak, ortaokul ve liselerde kod yazma, interneti ve sosyal medyayı güvenli olarak kullanma eğitimlerinin müfredata eklenmesinin gerekli olduğuna inanıyoruz."

mik dünyanın birlikte hareket etmesinin önemini vurguladık.

Geçtiğimiz sene Başbakanımız Binali Yıldırım'ın katılımları ile "Bilişim ve Demokrasi" başlığı ile Bilişim 2016 -33. Ulusal Bilişim Kurultayı'nı büyük bir katılımla gerçekleştirdik. Başbakanımız 2017 yılını "Bilişim ve Demokrasi" yılı ilan etti. Bu sene de Kalkınma Bakanımız Lütfi Elvan'ın katılımı ile Bilişim 2017-34. Ulusal Bilişim Kurultayını 20-21 Aralık tarihlerinde Ankara'da gerçekleştirdik.

"Geleceğimizi Kodlayan Çocuklarımız Olsun"

Türkiye'nin geleceği için 2018'de gençleri ve çocukları bilişim sektörüne kazandıracak bir kampanya gerçekleştireceğiz.

Dünyada teknoloji baş döndürücü hızla ilerliyor. Bir kuşak önce kurduğumuz hayalleri bizden sonraki kuşaklar hayata geçiriyordu. Artık günümüzde hayal ettiğimiz gelişmelerin üç ya da beş yıl sonra gerçekleştiğini görüyoruz. Otuz yıl içerisinde günümüzün popüler olan meslekleri teknolojinin gelişmesi ile yok olacak. Yakın bir zamanda savcıya, öğretmene hatta doktora bile ihtiyaç duymayacağız. Bu da gelecekte istihdamın değişeceğine, çocuklarımızın şu anda adını bile duymadığımız mesleklere sahip olacağını gösteriyor. Anne ve babalar olarak bu gelişime ve değişime ayak uydurmamız gerekiyor.

TBD olarak çocuklarımızın yazılım kodlamasını küçük yaşlarda öğrenmesini sağlamak istiyoruz. Çocuklarımızı teknoloji tüketen değil, teknoloji üreten çocuklar olarak yetiştirmek istiyoruz. Temel amacımız ise geleceği tasarlayan, özgür düşünen çocuklar yetiştirmek. Çocukların robotları yaratan, o robotlara yazılımlar yazan çocuklar olarak yetişmesi lazım. Onun içinde çocukların özgür, araştırıcı bir anlayışla yetişmeleri gerekiyor. Bunu yapabildiğiniz zaman o robotları yaratabilirsiniz. O robotları hareket ettiren yazılımları yapabilirsiniz yahut da akıllı kentleri. Akıllı dediğimiz her şeyin arkasında bir yazılım var. Bu çocuklar aslında kendi geleceklerinin yanında ülkemizin geleceğini de kodlayacak. Ülkemizin teknoloji çağını yakalayıp, bilişim çağında üreten bir ülke olma şifresi bugünün çocuklarına kodlama öğretmekle başlayacak.

Geleceği Şekillendirecek Olan Çocuklara Kodlama Eğitimi Verilmesi

Siber güvenlikte en zayıf halkanın ve aynı zamanda da en önemli faktörün insan olduğu bilinciyle; insanları eğitmek, bilinçli ve etik bilişim kullanıcıları haline getirmek amacıyla ilköğretimden başlayarak, ortaokul ve liselerde kod yazma, interneti ve sosyal medyayı güvenli olarak kullanma eğitimlerinin müfredata eklenmesinin gerekli olduğuna inanıyoruz.

2025 yılında bir trilyon cihazın internete bağlanacağı belirtiliyor. Bu cihazları internete bağlayacak ve bu cihazlarla interneti şekillendirecek olanlar bugünün

im 2017

LİŞİM KURULTAYI

-Gelişim

ital Dönüşüm







tbd.org.tr - bilisim.org.tr

çocukları olacaktır. Bu nedenle özellikle gelişmiş ülkeler, ulusal ve uluslararası alanda çocuklara yönelik "kodlama hareketleri" başlatmışlardır. TBD olarak "Geleceği Kodlayan Çocuklar Projesi" üzerinde çalışıyoruz. Bu projenin amacı;

- Türkiye'nin 7 bölgesinde 8-14 yaşları arasında 20.000 çocuğa; dijital okuryazarlık, kodlama, mobil uygulama geliştirme, oyun geliştirme ve web site geliştirme öğretilerek çocukların sistematik düşünme, problem çözebilme, olaylar arasındaki ilişkileri görebilme, yaratıcı düşünebilme gibi yetiler kazanmalarına yardımcı olmak.
- Kodlamanın fen bilimlerini kavramada etkili olduğunu göstermek.
- Çocukların bölgelerin özelliklerini (turizm, hayvancılık, el işi vs.) kodlamada kullanarak, bölgenin dijital dönüşüme taşınmasında farkındalığın gelişmesine etken olmak.

Ayrıca TBD olarak da üzerimize düşen görevleri yerine getirmek ve farkındalık yaratmak amacıyla sosyal sorumluluk projesi kapsamında şehit ve gazi çocuklarının rehabilitasyonu ve topluma kazandırılmaları amacıyla, mobil uygulama geliştirme (kod yazma eğitimi) atölyesi gerçekleştirilecektir. Bu atölyenin ilk çalışması kurultay programında yer almaktadır. Söz konusu atölye çalışmasında, MIT tarafından geliştirilen APP Inventor aracı kullanılarak sürükle bırak yöntemiyle çocuklar Android tabanlı mobil uygulamalarını geliştirecektir. Geliştirilecek uygulamalar içerisinde animasyonlar barındıran oyun türünde uygulamalar olacağı gibi, matematiksel işlemler yapılabilen derslere yardımcı uygulamalar da olacaktır.

Ayrıca TBD'nin iki önemli projesi hakkında da kısaca bilgi vermek istiyorum.

Korkma Konuş Projesi (2KP)

Korkma Konuş Projesi, çevrim içi kadın ve çocuk istismarına yönelik (Cinsel Tacizler Konusunda) olarak çocuklar, kadınlar, aileler, kamu görevlileri ve toplumun tüm kesimlerinde farkındalık oluşturmayı ve söz konusu paydaşlarla çocuk istismarını algılama, ihbar etme ve etkin olarak yasal mücadele edebilme amacıyla eğitim verilmesini hedeflemektedir.

Söz konusu eğitimlerin sadece çocuklara değil, ebeveynlere ve bu konuda görev yapan (Öğretmen, Polis, Savcı, Hâkim, Avukat, Doktor, Sağlık Bakanlığı Temsilcisi, Aile ve Sosyal Politikalar Bakanlığı Temsilcisi vb.) profesyonellere de verilmesi çocuk istismarını engellemeye yönelik yürütülen faaliyetlerin etkinliğini arttıracaktır. Proje kapsamında Ankara'da panel ve eğitimlerin gerçekleştirileceği bir adet konferans, çocuk tacizlerinin en yoğun olduğu ve çocuk izleme merkezi bulunan iller arasından pilot olarak seçilen 3 ilde ise çalıştay ve eğitimler düzenlenecektir. Bu eğitime katılanlara "Çocuk Meleği Brövesi" verilecek ve çocuk meleklerin bu eğitimi kendi bölgelerinde vermeleri teşvik edilecektir. Ayrıca söz konusu eğitimler dijital ortama aktarılacak ve çevrim içi olarak internet altyapısı üzerinden verilerek projenin sürdürülebilirliği sağlanacaktır.

Bu proje ile ilgili altyapı oluşturulmuş, içerikler belirlenmiş ve proje önerisi hazır hale getirilmiştir. Sponsor bulma faaliyetleri devam etmektedir. En kısa sürede hayata geçirilecektir.

Siber Güvenlik Elemanlarına Ait Ulusal Meslek Standardının Hazırlanması

Mevcut durumda siber güvenlik alanında Mesleki Yeterlilik Kurumu (MYK) tarafından tanımlı olan herhangi bir "Ulusal Meslek Standardı" ve "Ulusal Yeterlilik" bulunmamaktadır. Kamusal ve Sektörel SOME'ler başta olmak üzere bilişim ve siber güvenlik sektörlerinin ihtiyaçları göz önünde bulundurulduğunda siber güvenlik konusunda ihtiyaç duyulan meslek grupları için Ulusal Meslek Standardı'nın acilen hazırlanması ulusal kapasitenin arttırılmasına ve SOME'ler başta olmak üzere ihtiyaç duyulan siber güvenlik uzmanı açığının kapatılmasına önemli kazanımlar sağlayacaktır. Bu konuda MYK ile görüşülmüş ve siber güvenlik alanındaki meslek grupları için (6) adet Ulusal Meslek Standardı'nın hazırlanması görevi TBD'ye verilmiştir.

2018 yılı başında tüm hazırlıkların ta-



mamlanarak projeye başlanılması hedeflenmektedir.

CyberMag: 20-21 Aralık 2017 tarihinde Sheraton Ankara Hotel & Convention Centre'de gerçekleştirilecek olan TBD 34'üncü Ulusal Bilişim Kurultayı'nın teması Başbakanımızın talimatlarına uygun şekilde "Bilişimle-Gelişim: Türkiye'de Dijital Dönüşüm" olarak belirlenmiştir. Öncelikle bu etkinliğin amacı, ülkemize ve sektöre katkıları nelerdir?

Rahmi Aktepe: 20-21 Aralık 2017 tarihinde Sheraton Ankara Hotel & Convention Centre'de gerçekleştirdiğimiz TBD 34'üncü Ulusal Bilişim Kurultayının teması Başbakanımızın geçen yıl yapılan 33'üncü kurultayımızdaki talimatlarına uygun şekilde "Bilişimle-Gelişim: Türkiye'de Dijital Dönüşüm" olarak belirlenmiştir.

Kurultayın düzenlenmesi ve temasının belirlenmesindeki ana amaçlarımız;

Dijital Olgunluk Seviyesinin Yükseltilmesi;

Bilişim ekosisteminde ihtiyaç duyulan kabiliyetlerin geliştirilmesi amacıyla ulusal seviyede dijital dönüşüm ihtiyaçlarının belirlenmesi, kamu kurumlarının ve sektörün dijital olgunluk seviyesinin yükseltilmesine yönelik inovatif çözümlerin ve ulusal e-devlet politikalarının yer aldığı stratejilerin hazırlanması ve tek elden merkezi olarak yürütülmesi, izlenmesi ve değerlendirilmesi önemlidir. Vatandaşlar için sayısal okuryazarlık oranının arttırılmasını hedefleyen TBD, kamu kurumları ile özel sektör için de dijital olgunluk seviyesinin arttırılmasını ve dijital ekonominin büyümesini amaçlamaktadır.

Kurultayda konunun uzmanları ve akademisyenler tarafından kurumların dijital olgunluk seviyesinin ölçülmesine ve yükseltilmesine yönelik politika ve stratejilerin ortak akıl ile oluşturulmasına yönelik çalışmalar yapıldı.

Dijital Ekonominin Önemi;

Dijital ekonomi, hükümetler diğer bir deyişle politika yapıcılar için çok önemlidir. OECD üyesi 34 ülkeden 27'si bu alanda ulusal stratejilerini yayımlamıştır. AB ise Sayısal Tek Pazar ile vatandaşların ve kurumların dijital hizmetlere çok daha hızlı ulaşmasını ve daha verimli olarak kullanmasını hedeflemektedir. Ülkemizde de halen gelişmekte olan dijital ekonominin sürdürülebilirliğine yönelik altyapılar oluşturulmalı ve farkındalık yaratılmalıdır.

Nitelikli İnsan Kaynağının Yetiştirilmesi;

Dijital dönüşüm ile birlikte, önümüzdeki beş yıl içerisinde bugün önemli olarak

değerlendirilen becerilerin üçte birinin değişeceği, iş süreçlerinin ve iş yapış biçimlerinin değişime uğrayacağı, bazı mesleklerin tamamen yok olacağı, buna karşın bugün hiç bilinmeyen yeni meslek dallarının ortaya çıkacağı (Robot Veterineri, Drone Bekçisi, Veri Mühendisliği vb.) tahmin edilmektedir. Diğer taraftan, ülke seviyesinde sürdürülebilir siber güvenliğin sağlanması ve ulusal kapasitenin arttırılması amacıyla ihtiyaç duyulan yenilikçi ve özgün teknolojilerin geliştirilmesi amacıyla nitelikli insan kaynağına gereksinim duyulmaktadır.

Ulusal Siber Güvenlik Ekosisteminin Geliştirilmesi;

Siber Güvenlik Eylem Planları'nın etkin olarak uygulanması ve gerçekleştirilmesinin izlenmesi, sonuçlarının tarafsız olarak ölçülmesi ve raporlanması Ulusal Siber Güvenlik Ekosisteminin geliştirilmesine, sürdürülebilirliğine ve güçlendirilmesine önemli kazanımlar sağlayacaktır. Ayrıca siber güvenlik ekosisteminin çerçevesinin oluşturulması ve yasal düzenlemelerin yapılması çok önemlidir.

Diğer taraftan sürdürülebilir siber güvenlik ekosisteminin geliştirilmesi ulusal seviyede siber güvenlik kapasitesinin arttırılmasına ve toplumun tüm katmanlarında farkındalık yaratılmasına olanak sağlayacaktır. Bu konuda yapılması gereken eylemler;

1. Ekosistemin Yeniden Yapılandırılması;

Söz konusu ekosistem içerisinde; başta ekosistemi yöneten politika ve stratejilerini belirleyen icra yeteneğine sahip bir makam olmak üzere müşteriler, tedarikçiler ile teknoloji, ürün ve hizmetlerin geliştirilmesine katkı sağlayan sektör paydaşları, standardizasyon ve sertifikasyon kuruluşları, akreditasyon ve eğitim tesisleri, üniversiteler ve STK'lar başta olmak üzere tüm paydaşlar yer almalıdır. Söz konusu paydaşlar arasında iletişimi ve uyumu sağlamak için yasal çerçeve oluşturulmalıdır.

2. Siber Güvenlik Kurulunun Etkinleştirilmesi;

Siber Güvenlik Kurulu tarafından yürütülen faaliyetlerin etkinleştirilmesi ve sürdürülebilir kılınmasına ihtiyaç duyulmaktadır. Bu nedenle kamu, özel sektör, STK'lar ve üniversitelerden uzman kişilerin görevlendirileceği teknik çalışma gruplarının ve izleme komitelerinin oluşturulmasına acil ihtiyaç bulunmaktadır.

Kamu kurum ve kuruluşları ile özel sektör, STK'lar, üniversiteler ve vatandaşlar arasında siber güvenlik konularında ortak akıl oluşturulabilmesi amacıyla "Sivil İnisiyatifler" oluşturulmalı ve sivil inisiyatiflerin moderatörleri ulusal siber güvenlik kurulunun doğal üyesi olmalıdır.

3. Yerli Sektörün Güçlendirilmesi;

Türkiye suçlar ve saldırılar açısından her zaman hedef seçilen ilk 10 ülke arasında yer almaktadır. Türkiye aynı zamanda siber saldırı yapan ülkeler arasında ilk sıralarda gözükmektedir. Kamu kurumları ve/veya kritik altyapılarda kullanılan çözümlerin yaklaşık %97'sinin yabancı (ithal) menşeili olduğu bilinmektedir.

Yerli siber güvenlik ürün, sistem, çözüm ve hizmetlerinin milli kabiliyetler ile özgün olarak geliştirilmesi, yerli ve özgün çözümlerin kritik altyapılarda kullanımının teşvik edilmesi ve yaygınlaştırılması ulusal seviyede siber güvenlik kapasitesinin geliştirilmesine önemli katkılar sağlayacaktır.

Siber güvenlik alanında milli kabiliyetler ile hangi teknolojilerin geliştirilmesine ihtiyaç olduğu ve bu ihtiyaçların önceliklendirildiği "Ulusal Siber Güvenlik Teknoloji Yol Harita"larının oluşturulması ve bu bilgilerin sektör ile paylaşılması kaynak israfının engellenmesine ve hem sektörün hem de ulusal seviyede siber güvenliğin sürdürülebilirliğine önemli kazanımlar sağlayacaktır.

4. Standartlara Uyum ve Ürün Sertifikasyonu;

Siber güvenlikte en önemli konu standartlara uyumdur. Siber güvenlik standartları, kullanılan güvenlik sistem ve/veya ürünlerine yönelik oluşabilecek risklerin belirlenmesi ve gerekli olan risk analizlerinin sağlıklı ve maliyet etkin olarak yapılabilmesine olanak sağlamaktadır.

İlgili STK ve sektörün de katılımıyla kamu kurum ve kuruşları ile kritik altyapılarda kullanılacak olan bilişim teknolojileri ve siber güvenlik ürün, sistem ve hizmetlerine yönelik asgari güvenlik iş yerleri tanımlanmalı, standartlar oluşturulmalı ve ürün sertifikasyon süreçleri belirlenmelidir. Ayrıca rekabete açık yapıda sertifikasyon test merkezleri oluşturulmalıdır.



5. Ulusal Kapasitenin Arttırılması İçin Hedef Odaklı Tatbikatların Yapılması;

Kamu kurumları ile kritik altyapıların siber saldırılara karşı dirençlerinin arttırılması, siber saldırı sonrası ise sistemlerin en kısa sürede hizmete alınabilmesi, ulusal kapasitenin arttırılması için düzenli olarak siber güvenlik tatbikatları yapılmalıdır.

Tatbikatlar sektör odaklı olmalı ve katılım zorunlu hale getirilmelidir. Tatbikat sonuçları kamuya açık olmalı ve bu sonuçlar analiz edilerek her kurum için ev ödevi çıkarılmalıdır.

6. Siber Güvenlik Eğitimleri;

Siber güvenlik kapasitesinin arttırılabilmesi için toplumun her kademesinde siber güvenlik farkındalığı oluşturulmalıdır. Bu amaçla ilk ve orta öğretimden başlamak üzere her seviyedeki eğitim kurumlarında siber güvenlik farkındalık eğitimleri verilmelidir. Ayrıca siber güvenlik alanında ihtiyaç duyulan nitelikli uzman kişilerin yetiştirilebilmesi amacıyla özellikle siber güvenlik ve teknolojileri eğitimleri üniversite müfredatına eklenmelidir.

Siber güvenlik alanında 30.000 olarak açıklanan yetişmiş insan gücü açığının kapatılmasına yönelik olarak kısa, orta ve uzun vadeli hedeflerin belirlenmesi ve bu hedeflere göre uzman açığının giderilmesi şarttır.

Kurultayda uzmanlar, akademisyenler ve STK yetkilileri tarafından söz konusu ekosistemin geliştirilmesine ve sürdürülebilirliğine yönelik konular teknoloji, süreç ve insan boyutuyla analiz edildi ve yapılması gereken eylemler masaya yatırıldı.

Yerli ve Yenilikçi Teknolojilerin Geliştirilmesi;

Düşük gecikmeli ve yüksek hızlı veri iletişiminin yanı sıra büyük miktarda verinin aynı anda işlenmesine olanak sağlayan ve düşük güç tüketimine sahip 5G ve ötesi teknolojiler kendi güçlü ekosistemlerini yaratarak, kalkınmaya getireceği katkıyla yeni bir yaşam tarzı oluşturma konusunda farklı boyutlar ve fırsatlar yaratacaktır.

Yerli üretim yapan yazılım ve donanım firmalarının daha fazla teşvik edilmesi ve yerli ürün ekosisteminin geliştirilmesinin sağlanması amacıyla çeşitli yasal düzenlemeler yapılmış ve bilişim teknolojileri ile yazılım sektörü sanayici tanımına alınmıştır.

CyberMag: Konferans konu başlığından yola çıkarak, Türkiye dijital dönüşümün neresinde? Dijital dönüşümü, kültürel dönüşümle taçlandırmak için; kamu, üniversite, finans kuruluşları, sektör temsilcileri ve her biri sektöre öncülük eden sivil toplum kuruluşları dijital değişim ve dönüşümün ana aktörleri olarak üstlenmesi gereken görevler nelerdir?

Rahmi Aktepe: Her şeyin dijitalleştiği, dünya nüfusunun neredeyse yarısının online olduğu günümüzde Türkiye hızla gelişen ülkeler arasında. Fakat, şirketlerin yüzde 95'i hala dijital dönüşüm sürecini tamamlayamadı.

Dijital dönüşüm sadece teknolojik yatırımlar değil. Dönüşüm, insan kaynaklarından iş süreçlerine hatta yönetim kurullarına kadar bir toplu kültürel değişimi, yeni bir yapı oluşturmayı kapsıyor.

Dijital ekonominin hız kazanması için inovasyon ve AR-GE yatırımları çok önemli.

Dijital dönüşümü, kültürel dönüşümle taçlandırmak için; kamu, özel sektör, üniversite, finans kuruluşları, holdingler, sektör temsilcileri ve her biri sektöre öncülük eden sivil toplum kuruluşlarının el ele vermesi ve iş birliği içinde olması gerekiyor.

Dijital gelişimi ülkemize bir yatırım olarak değerlendirmemiz gerekiyor. Mobil cihaz kullanımında artış sağlamak, mobil internet kullanımını da arttıracağı için, dijitalleşmede önemli bir adım.

CyberMag: Konferansınızda toplamış olduğunuz bildiriler ile ülkemizin bilimsel gelişimine katkıda bulunuyorsunuz. Bildirilerin yayımlanması için onay ve eleme sürecinde nelere dikkat ediyorsunuz?





Rahmi Aktepe: Bilişim 2017-34. Ulusal Bilişim Kurultayı'nda akademik ve teknoloji uygulama bildirilerinin sunulacağı oturumlar da düzenliyoruz. Akademik ya da teknoloji uygulama konularında sunulacak her bir bildiri etkinliğimize önemli bir katkı sağlamakta.

Gönderilen bildiriler çok değerli hakemlerimiz tarafından titizlikle değerlendiriliyor.

Bildiri başvuruları en az iki Bilişim 2017 Bildiri Değerlendirme Kurul Üyesi tarafından değerlendiriliyor, kabul edilen bildiriler konu başlıklarına göre sınıflandırılarak sunuluyor.

Sunulan bildiriler Kurultay Bildiriler Kitabı'nda yer alıyor.

CyberMag: Etkinliğiniz panel başlıklarına baktığımızda geniş yelpazede sektörün tüm sorunlarını ele aldığınızı görüyoruz. Dergimizin de faaliyet alanı göz önünde bulundurulduğunda "Sürdürülebilir Siber Güvenlik ve Ulusal Stratejiler" konulu panelden yola çıkarak, ulusal güvenlik açısından siber güvenliğin önemi nedir? Türkiye diğer ülkelere kıyasla ne durumda?

Rahmi Aktepe: Siber güvenliğin içinde teknoloji, insanların eğitimi ve kanunlar var. Son yıllarda siber güvenliğin bu kadar sık kullanılmasının nedeni, artık her şeyin sayısallaşması ve bilgi teknolojilerinin günlük hayatımızın bir parçası olması nedeniyle, bireyler, kurumlar ve devletler her türlü tehdide açık hale dönüştüler. Bunun için gelişmiş ülkelerin, kara, hava, deniz ve uzay platformlarının ardından beşinci savaş boyutu olarak "siber ordular" kurmaya başladılar.

Siber güvenlik sadece askeri güçlerin alacağı önlemlerle sağlanabilecek bir olgu değil olaya her alanı kapsayacak şekilde bütüncül bir bakış açısıyla yaklaşmak gerekiyor.

Kamuda, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Kurumsal Siber Olaylara Müdahale Merkezi (SOME) yapıları bulunuyor.

Ülkemizin yarınlarını garanti altına alacak ve siber güvenliğini sağlayacak ihtiyaç olunan nitelikli insan kaynağından çok uzakta olduğumuz bir gerçek. Ülkemizde 10 bine yakın bir siber güvenlik uzmanı açığı olduğu belli. Fakat ne yazık ki bugün siber güvenlik konusunda kurumsal bir eğitimimiz yok. Şu anda müfredatlara baktığımızda sadece birkaç üniversitemizde var. Onun dışında Mesleki Yeterlilik Kurumu'nda henüz uzmanlık sınıfı olarak tanımlanmış bir alan da değil. Sadece Türk Standartları Enstitüsü'nün yılda 2 kez açılan beyaz şapkalı hacker programında çeşitli sertifika programları var. Ulusal seviyede nitelikli bir siber güvenlik uzmanı yetiştirme programının ivedilikle hayata konulmasının çok faydalı olduğunu düşünüyoruz.

Son olarak siber güvenlikte milli çözümler olmazsa güvende olmaz... Bu nedenle insan kaynağına ihtiyacımız var. 2019 için dünyada 2 milyon siber güvenlik uzmanı açığı var.

Bize düşen payın da en az 20 bin olduğunu düşünüyoruz. Milli çözümler üretmeli ve nitelikli siber güvenlik uzmanı yetiştirecek şekilde eğitim sistemimizi planlamalıyız.

CyberMag: TBD olarak, bilgi güvenliği konusunda çalışma yürüten sivil toplum kuruluşlarına örnek olarak gösterilebilirsiniz. Bu durum göz önünde bulundurulduğunda, sektör üzerinde bir sinerji oluşturmak ve farkındalık yaratmak adına sivil inisiyatif organlarına düşen görevler nelerdir?

Rahmi Aktepe: Tüm sektör dernekleri kamu-özel sektör işbirliğini oluşturmada köprü olmalı ve geliştirilecek projelerde katalizör rol üstlenmelidir.

TBD olarak diğer sivil toplum kuruluşları ile işbirliği içerisindeyiz. Yaptığımız dikey sektör etkinlikleri ile de meslek odaları, derneklerle işbirliği içerisinde çalışmalarımızı sürdürüyoruz. Çalışma grupları kuruyoruz, meslek içi eğitim programlarımız var.

Sektörel raporlarımız, eğitimlerimiz, seminerlerimiz ve kongrelerimiz ile farkındalık oluşturup, insanları bilinçlendirmeye çalışıyoruz.

Bilişimle ilgili her türlü uygulama ve yasal düzenlemeler konusunda görüş oluşturup, ilgililerin dikkatine sunuyoruz, plan ve politikaların oluşmasına katkı veriyoruz.

CyberMag: CyberMag, siber dünyadaki riskler ve siber güvenlik konusuna odaklanmış Türkiye'nin ilk basılı ve elektronik dergisi olarak farkındalığı artırmayı ve insanları bilgilendirmeyi amaç edinmektedir. Bu amaçla yola çıkan ve yayın hayatına bir seneyi aşkın bir süredir devam eden CyberMag hakkında düşünceleriniz nelerdir?

Rahmi Aktepe: Öncelikle siber güvenlik konusunda sektörün nabzını tutarak, insanları bilinçlendirdiğiniz için teşekkür ediyoruz. Böyle bir ihtiyacın tarafınızca doldurulduğuna inanıyoruz.

Dergiye emek veren herkesi kutlar, yayın hayatınızda başarılar dileriz.



2018 Yılına Damgasını Vuracak Siber Güvenlik Trendleri

McAfee, 2018 yılında dikkat edilmesi gereken siber güvenlik trendlerini McAfee Labs 2018 Tehdit Tahminleri Raporu'nda açıkladı. Hızlı bir evrimden geçen yeni nesil fidye yazılımları, güvenlik risklerini beraberinde taşıyan sunucusuz uygulamalar, tüketici gizliliğini hiçe sayan bağlantılı ev cihazları, çocuklar tarafından üretilen dijital içeriklerin gelecekte yaratabileceği riskler ve makine öğrenimi ile hızlanan siber güvenlikte 'silahlanma yarışı' raporun başlıca öne çıkan konuları arasında…

Dünyanın lider internet güvenlik şirketlerinden biri olan McAfee, 2018 yılını şekillendirecek 5 temel trendi paylaştığı McAfee Labs 2018 Tehdit Tahminleri Raporu'nu yayımladı. Bu yıl raporda fidye yazılımlarının evrimi, sunucusuz uygulamaların siber güvenliğe olan etkileri, kurumların tüketicileri evlerinde izlemelerine olanak tanıyan teknolojilerin tüketici gizliliğine etkileri, kurumların çocuklar tarafından geliştirilen içerikleri toplaması sonucu uzun dönemde oluşabilecek riskler ve siber güvenlik uzmanları ile siber suçlular arasındaki makine öğrenimi ile yeni inovasyonlar yaratma yarışı yer alıyor.

2017 yılındaki siber tehditlerin artan gücüne dikkat çeken McAfee Baş Teknoloji Sorumlusu Steve Grobman; "Bu yıl fidye yazılımlarının geçirdiği evrim, tehditlerin ne denli agresif bir şekilde kendini yeniden yaratabileceğini ve siber güvenlik uzmanlarının başarılı çalışmalarına siber suçluların ne kadar büyük bir hızla uyum gösterdiklerini ortaya koydu. Siber güvenlik uzmanları makine öğrenimi, derin öğrenme ve yapay zekâ gibi yeni nesil teknolojilerle geleceğin güvenlik önlemlerini yaratırken; siber suçlular da bu teknolojilere karşı güçlü teknikler icat ediyor ve uyguluyor. Siber güvenlikte teknolojinin gücüyle beslenen insan zekâsı, siber güvenlik ekipleri ile siber saldırı düzenleyenler arasındaki yarışta kazanmayı garantileyen faktör olmaya devam edecek" dedi.

Siber suç ve IT evrimine dair güncel trendleri inceleyen rapor, McAfee Labs, McAfee Gelişmiş Tehdit Araştırma Birimi ve McAfee CTO birimi başta olmak üzere kurum içinden pek çok fikir önderinin bilgisi, deneyimi ve görüşlerine yer veriyor. Kurumların işlerini geliştirmeleri ve daha iyi güvenlik önlemleri almaları için yeni nesil teknolojilere dair verileri paylaşıyor ve geleceğe ışık tutuyor.

Siber Güvenlik Ekipleri ve Siber Suçlular Arasındaki "Silahlanma Yarışı" Kızışıyor

Makine öğrenimi, güvenlik açıklarını, şüpheli davranışları ve zero-day saldırılarını tespit etmek ve düzeltmek üzere devasa boyuttaki verileri işleyebilir ve büyük



ölçekli operasyonlar gerçekleştirebilir. Aynı zamanda siber suçlular da koruma tekniklerinden öğrenimler elde etmek, tehdit tespit modellerini etkisiz hale getirmek ve siber güvenlik uzmanları güvenlik açıklarına bir yama geliştiremeden bu açıkları kendi çıkarları için kullanmak gibi pek çok konuda makine öğreniminden yararlanıyor.

Bu yarışı kazanmak için kurumların insan gücünün stratejik zekâsından yararlanarak makine tabanlı kararlar alması ve tehditlere karşı yanıtlarını buna göre düzenlemesi gerekiyor. Ancak bu şekilde kurumlar, saldırıların hangi şekillerde gerçekleşebileceğini, bu yöntem daha önce hiç uygulanmamış olsa dahi anlayabilir ve öngörebilir.

Fidye Yazılımları Değişimden Geçiyor

Geleneksel fidye yazılımı yöntemleri, daha güçlü güvenlik önlemleri, daha bilinçli insan kaynağı ve stratejiler sayesinde kârlılığını kaybediyor. Siber suçlular da geleneksel yöntemler yerine daha kârlı olan yüksek net-değerine sahip kişileri, bağlı cihazları ve kurumları hedef almaya başlıyor.

Bu dönüşüm ile birlikte fidye yazılımları bireylerin dolandırılması yerine, kurumlara siber şantaj yapılması ve yıkıcı etkiler yaratılmasına kadar uzanan yeni hedefler için kullanılmaya başlandı. Bu doğrultuda siber sigorta pazarı da hızla büyüyor.

Sunucusuz Uygulamalar Saldırıya Açık Alanı Genişletiyor

Sunucusuz uygulamalar sayesinde bugün hizmetlerin daha hızlı faturalandırılması gibi pek çok işi daha geniş bir eksende yönetmek mümkün. Ancak bunlar, yetki yükseltme (privilege escalation) ve uygulama bağlantıları (application dependencies) kullanılarak gerçekleştirilen saldırılara açıklardır. Ayrıca sunucusuz mimarinin ölçeklendirme yapamayarak maliyetli hizmet kesilmelerine neden olan 'brute force' DoS (Denial of Service) saldırılarına ve bir ağ içerisindeki veri transferine yapılan saldırılara uğramaları da daha muhtemel.

Bu nedenle sunucusuz uygulamalarda işlev geliştirme ve dağıtım süreçlerine gerekli güvenlik önlemleri entegre edilmeli, ölçeklenebilirlik özellikleri eklenmeli ve ağ trafiği VPN ve şifreleme ile koruma altına alınmalı.

İnternet Bağlantılı Ev Cihazları İle Kişisel Bilgiler Açığa Çıkıyor

Şirketler pazarlama faaliyetlerinin başarısını artırmak üzere cihaz sahiplerinin satın alma ihtiyaçları ve tercihlerini anlamak için tüketici davranışlarını daha yakından inceleme eğilimi taşıyor. Tüketiciler nadiren gizlilik sözleşmelerini okuduğu için de şirketler bu sözleşmeleri sürekli olarak daha fazla bilgi edinmek için değiştirmek ve bu bilgileri gelirlerini artırmak üzere kullanmaya yöneliyor.

McAfee, mevcut yasaları ihlal edip karşılığında ceza ödeyerek bu tür eylemlere devam eden ve bu sayede kâr sağlamayı hedefleyen şirketler için yeni yaptırımlar uygulanacağına inanıyor.

Çocuklara Ait Dijital İçerikler Tehdit Oluşturuyor

Kullanıcı uygulamalarının başarısını artırmak için şirketler genç kullanıcılar tarafından geliştirilen içerikleri toplama konusunda her geçen gün daha rekabetçi oluyor. 2018 yılında aileler çocuklar tarafından üretilen dijital içeriği kendi çıkarları için kullanan kurumlar hakkında daha bilinçli olacak ve bu tür uygulamaların uzun vadede çocukları için yaratabileceği potansiyel risklerin farkında olarak hareket edecekler.

McAfee, geleceğin yetişkinlerinin 'dijital yüklerinden' dolayı sıkıntı yaşayabileceğine inanıyor. Çünkü bugün çocuklar ve aileleri, sınırları henüz kesin kurallarla belirlenmemiş olan bir ortamda, kişisel bilgilerin iç içe geçmesini sağlayan kullanıcı ara yüzlerine sahip uygulamalarda geliştirilen kullanıcı içeriklerinin şirketler tarafından gelecek dönemde sömürülebileceğinin farkında değiller.

Yoğun rekabetin yaşandığı uygulama evreninde, geleceği öngören uygulama ve hizmet sağlayıcıları marka itibarını korumanın öneminin farkına varacak. Uygulama bağımlılığı yaratmak için agresif yöntemler geliştirmek yerine ailelerle birlikte çalışmayı ve bu eğitim seferberliğinde onlara yol arkadaşı olmayı seçecek.

SİBER ZORBA OLMA!
#FARKINAVAR

Samsung Electronics Türkiye, Bilgi Teknolojileri ve İletişim Kurumu (BTK) iş birliğiyle siber zorbalığa karşı "Siber Zorba Olma! #farkinavar" hareketini başlatıyor. Çocukların, gençlerin ve ailelerin siber zorbalığa karşı bilinçlendirilmesi amacıyla yıl boyunca verilecek eğitimlerin yanı sıra 13 Aralık'ta sosyal medya hareketi başlatıldı.

"Birlikte İyi Gelecek" vizyonuyla hareket eden Samsung Electronics Türkiye, Bilgi Teknolojileri ve İletişim Kurumu (BTK) iş-birliği ile siber zorbalık konusunda çocukların, gençlerin, ailelerin ve öğretmenlerin farkındalığını artırmayı hedefleyen "Siber Zorba Olma! #farkinavar" hareketini başlatıyor.

Elektronik ortamda bir birey veya grubun, diğerlerine yönelik kasıtlı biçimde gerçekleştirdiği aşağılama, iftira, dedikodu, taciz, tehdit, utandırma ve dışlama gibi rahatsızlık verici eylemleri ifade eden "siber zorbalık" kavramı her gün binlerce çocuk ve gencin fiziksel ve psikolojik zarar görmesine sebep oluyor.

Samsung ve BTK iş birliği ile yürütülen "Siber Zorba Olma! #farkinavar" kampanyası dâhilinde pilot 20 okul ile başlayacak eğitimlerde çocukların, gençlerin, ailelerin ve öğretmenlerin teknolojinin kötü amaçlı kullanımına karşı farkındalıklarının ve kişilik haklarının korunması konusunda duyarlılıklarının artması hedefleniyor.

Gençlerin teknolojiden en etkin şekilde faydalanmasının yanında, potansiyel zararlarını en aza indirmeyi amaçlayan "Siber Zorba Olma! #farkinavar" hareketini duyurmak amacıyla siber zorbalığa uğrayan gençlerin duygularını çarpıcı bir şekilde ortaya koyan ve Nejat İşler'in seslendirdiği dijital reklam filmi çekildi. Okullarda verilecek eğitimlerin yanı sıra siber zorbalığa dikkat çekmek için 13 Aralık günü Samsung Türkiye ve BTK sosyal medya hesaplarını karartıp, "Siber Zorba Olma!" sloganını #farkinavar hashtag'i ile paylaşarak herkesi sosyal medyadaki bu hareketin bir parçası olmaya davet etti.

Düzenlenen basın toplantısında konuşan Samsung Electronics Türkiye Başkanı DaeHyun Kim "Teknolojinin sunduğu birçok katma değerin yanında kötüye kullanımından doğan olumsuz sonuçlar da var; bunlardan biri de siber zorbalık. Samsung Electronics Türkiye olarak çocuklarımız ve gençlerimiz üzerinde psikolojik ve fiziksel anlamda yıkıcı etkileri olan bu sorunla ilgili tüm ülke genelinde farkındalık yaratmak için dijital bir film hazırladık. Sosyal



medya hesaplarımız üzerinden paylaşımı yapılacak filmimizle birlikte 13 Aralık günü tüm sosyal medya hesaplarımızı "Siber Zorba Olma!" görselimiz ile karartarak paylaşımlarımızda #farkinavar hashtagini kullanacağız. Projeyle ilgili yayılımı artırmak için tüm paydaşlarımızdan 13 Aralık günü sosyal medya hesaplarından "Siber Zorba Olma!" görselini paylaşarak projeye destek olmalarını istiyoruz" dedi.

Ülkemizde Siber Zorbalığa Maruz Kalanların Oranı Yüzde 20

"Biz kurum olarak gözbebeğimiz olan gençlerimizin ve çocuklarımızın kendi öz kültürünü, milli ve manevi değerlerini kaybetmeden en iyi şekilde teknolojik deneyime ve beceriye sahip olacak, gelecekte ben de varım diyecek şekilde yetkin ve donanımlı yetişmesini istiyor, bu yoldaki tüm çalışmaları destekliyoruz" diyen BTK Başkanı Ömer Fatih Sayan ise konuşmasını şöyle sürdürdü: "Siber zorbalık; bilgi iletişim teknolojileri aracılığıyla bir bireyin ya da grubun diğerlerine yönelik düşmanlık, korkutma, tehdit, sindirme, taciz amaçlı yazılı veya görsel iletileri kasıtlı ve düzenli bir şekilde gönderilmesi olarak karşımıza çıkıyor. Siber zorbalıkla mücadelede özellikle eğitimcilere, ailelere, gençlere, STK'lara, özel sektöre, ilgili kamu kurum ve kuruluşlarına çok önemli görevler düşüyor. 2010 yılından beri Türkiye'nin birçok ilinde öğrencilere, ebeveynlere, eğiticilere, adli ve mülki idari amirlere internetin bilinçli, güvenli ve etkin kullanımı konusunda verdiğimiz ve vermekte olduğumuz eğitim ve seminerlerde en önemli başlıklarımızdan biri de siber zorbalıkla mücadele. Bu mücadeleyi eğitim verdiğimiz 400 formatör öğretmen ve onların eğittiği 100 binin üzerinde öğretmen yürütüyor. Samsung ile birlikte yeni başlattığımız "Siber Zorba Olma! #farkinavar" hareketi kapsamında da önümüzdeki dönemde ailelere, öğretmenlere, öğrencilere ve eğiticilere siber zorbalık konusunda eğitim vermeyi planlıyoruz."

Ülkelere göre siber zorbalık oranlarını paylaşan Sayan, "İnternet kullanıcılarının Kanada'da yüzde 21'i siber zorbalığa maruz kalırken, yüzde 69'unun siber zorbalığa tanıklık ettiği görülüyor. İngiltere'de bu rakam yüzde 20 ve üzeri olarak kayıtlara geçerken, ülkemizde ise siber zorbalığa maruz kalanların oranı yüzde 20.

Amerika'da siber zorbalıkla mücadele etmek zorunda kalanların yüzde 20'sinin intiharı düşündüğünü açıklaması en ilginç verilerden biri. Bu rakamlar üstelik siber zorbalığa maruz kaldığını açıklayan kişilerden oluşuyor. Bunu açıklamamış kişiler de göz önünde bulundurulduğunda bu oranlar daha yükseliyor" açıklamasında bulundu.

Siber Zorbalıkta İstanbul İlk Sırada

Basın toplantısında konuşan, çocuk ve gençlerin internet kullanımı ve siber zorbalık konularında uzman Kocaeli Üniversitesi İletişim Fakültesi Gazetecilik Bölümü ve Bilişim Anabilim Dalı Başkanı Prof. Dr. Emel Baştürk Akca, siber zorbalığın yaygınlığını ve yarattığı sonuçları ortaya koymak amacıyla TÜBİTAK'ın desteği ile yürütülen araştırma projesinin sonuçlarına dikkat çekti: "Kocaeli Üniversitesi'nde TÜBİTAK'ın desteği ile yürütülen proje

kapsamında yedi ilde 7. ve 8. sınıfa devam eden 1400 öğrenci ile anket çalışması gerçekleştirildi. Siber zorbalık mağduru ve faili olma durumunun her ikisinde de ilk sırada yer alan İstanbul'da siber mağdur/kurban oranı yüzde 20'ye yaklaşırken, siber zorba olma oranı ise yüzde 15'i geçmektedir. Ayrıca siber zorbalık deneyimlerinin internet kullanım sıklığıyla doğru orantılı olduğu görülmüştür. Araştırmanın diğer bulguları öğrencilerin siber zorbalık konusunda yeterince farkındalığa sahip olmadığını, bu nedenle siber zorba ve kurban olma oranlarının daha yüksek olabileceğini göstermektedir. Çünkü siber zorbalık olarak tanımlanan eylemler sıralanarak sorular yöneltildiğinde siber zorba ve kurban olma oranlarının çok daha yüksek olduğu görülmektedir. Bu nedenle Samsung ve BTK öncülüğünde başlatılan "Siber Zorba Olma! #farkinavar" hareketi, siber zorbalığın önlenmesi ve çocuklar ve gençlere siber zorbalıkla baş etme becerisi kazandırılması açısından hayati önem arz ediyor."



Siber Zorbalık Hangi Şekillerde Karşımıza Çıkar?

- Mobil cihazlar aracılığı ile bireylerin görüntülerini izinsizce çekip paylaşmak,
- Sosyal ağlar ya da sohbet odaları gibi çevrimiçi ortamlarda bireyleri aşağılayıcı, alay edici, tehditkâr, cinsel taciz veya şiddet içeren mesajlar göndermek,
- Birinin kişisel bilgilerini rızası ve haberi olmadan sosyal medya aracılığıyla paylaşmak,
- Sosyal ağlarda birisi hakkında dedikodu yaymak,
- Bir kişiye ilişkin karalayıcı, aşağılayıcı web sayfaları hazırlamak,
- Başkası adına sahte hesap açıp, onun kimliğine bürünmek,
- Bir kişinin çevrimiçi ortamdaki tüm hesaplarını ısrarlı biçimde takibe almak,
- Ortak tanıdıkları etkileyerek hedef olarak seçilen bireyi arkadaş listelerinden silmelerini ve bloke etmelerini, yani sosyal olarak dışlamalarını sağlamak.

Kocaeli Üniversitesi'nin TÜBİTAK İle Yürüttüğü Siber Zorbalık Araştırmasına Dair Sonuçlar

- Araştırmaya katılan öğrencilerin % 90'ının Facebook'ta hesabı bulunuyor.
- % 11.64'ü sözlü siber zorbalığa maruz kaldığını; % 10.13'ü ise siber zorbalık yaptığını belirtmiş.
- Araştırmaya katılan öğrencilerin yaklaşık %56.5'i internette tanımadığı kişilerle konuştuğunu söylemiştir.
- Öğrencilerin %57.6'sı sosyal ağlarda "kullanıcıyı şikayet et/bildir" linkini kullanarak şikayette bulunduğunu ifade etmiştir. Öğrencilerin şikâyet etme nedenleri arasında ilk sırada "sözlü taciz" yer almaktadır.
- Siber ortamda, sözlü tacize maruz kaldığını belirten öğrencilerin oranı ise %25.4'tür.
- Araştırmaya katılan öğrencilerin %32,5'i siber zorbalığa maruz kalmaları halinde "kanıt içeriği silme" davranışını tercih etmektedir.
- Araştırmaya katılan kız öğrencilerin %16'sı, erkek öğrencilerin ise %30,5'i siber zorbalığa maruz kalmaları halinde "misilleme" yoluyla zorbalığa karşılık vermeyi uygun bulmaktadır.
- Çalışmanın dikkat çekici bulgularından biri de öğrencilerin siber zorbalığa maruz kalmaları halinde bunu öncelikle arkadaşları ile paylaşacaklarını ifade etmeleridir; (okul arkadaşına söylemek %41, çevrimiçi arkadaşa söylemek %31).
- Ailemle paylaşırım diyenlerin oranı %37, öğretmeniyle paylaşma oranı ise %15'tir. Bu durum ergenlerin siber zorbalık durumunda yetişkinleri öncelikli rehberler olarak görmediklerini ortaya koymaktadır.

Ebeveynler Siber Zorbalığı Önlemek için Neler Yapabilir?

- Çocuklarla siber zorbalık konusunda konuşmalı, onları yargılamadan dinlemeli ve başkalarına saygı konusunda çocuklara rol model olmalı,
- Çocukları siber zorbalığa karşı okulla işbirliği yapmaya teşvik etmeli,
- Çocuklarına siber zorbalığa maruz kaldığında bunu abartmak ya da yok saymak yerine nasıl mücadele edebileceklerini öğretmeli,
- Çocuklarını siber zorbalık vakalarında yetişkinlere, yasal kişi ve kurumlara bildirmeleri konusunda teşvik etmelidir.

2018'de Hazırlıklı Olunması Gereken 5 Bulut Bilişim Trendi

2018 yılında bulut üzerinde çalışan hizmetlerin kullanımındaki artışın katlanarak sürmesi, depolama ihtiyacının artması, nesnelerin interneti ve makine öğrenimi adaptasyonunun yaygınlaşması bekleniyor.

Türkiye'nin en hızlı büyüyen veri merkezi Radore, 2018 yılında bulut bilişime olan eğilimin hem Türkiye'de hem de dünyada artacağını duyurdu. Hem dünya çapında hem de Türkiye'de yapılan araştırmalar, şirketlerin 2018 eğilimlerini ortaya koyuyor.

Gartner'ın 2018 öngörülerine göre, mobil cihazların çalıştıracağı bulut tabanlı uygulamalar daha da artacak ve bağlantı hızı, bant genişliği, gecikme süreleri gibi ölçütler daha da belirleyici olacak. Türkiye'deki 400 KOBİ ile yapılan araştırmada KOBİ'lerin yüzde 71'inin bulut üzerinde herhangi bir çözüm kiralayacağını belirtmesi 2018 yılında da Türkiye'deki eğilimin artmaya devam edeceğini gösteriyor. IDC'nin 2021 öngörülerine göre, bulut bilişim hizmetlerine yapılan harcamalar ve buluta uygun donanım, yazılım ve hizmetlerin toplam hacmi 530 milyar doların üzerine çıkacak.

Nesnelerin interneti, video içeriklerin artışı ve sanal gerçeklik gibi teknolojiler nedeniyle verinin katlanarak arttığına dikkat çeken Radore Veri Merkezi Kurucusu ve Yönetim Kurulu Başkanı Zeki Kubilay Akyol, "Her yıl şirketlerin verisi ortalama iki katına çıkıyor. Bunca veri miktarı sebebiyle bulut bilişimin önemi her geçen gün artacak. 2018 yılında bulut bilişim hizmetlerine olan ilginin her zamankinden fazla olmasını bekliyoruz" dedi. Zeki Kubilay Akyol, 2018 yılında beklenen bulut bilişim eğilimlerini şu şekilde sıraladı:



- **Hizmet olarak yazılım(SaaS), altyapı ve platform harcamaları artacak:** Bulut bilişim hizmetlerinin sadeliği ve yüksek performansı işletmelere cazip gelecek.
- **Veri merkezlerinde sunulan depolama kapasitesi artacak:** Yapılan araştırmalara göre, dünya çapında toplam depolama kapasitesinin 1,1 ZB olması bekleniyor ki bu rakam 2017 yılının tam iki katı.
- **Nesnelerin interneti (IoT) ve yapay zekâ (AI) gerçek zamanlı veri ve bulut bilişim kullanımını tetikleyecek:** Yeni yılda anında 40 dilde çeviri yapan kulaklıklar, hizmet sektöründe yaygınlaşan robotlar hayatımıza girecek.
- **Daha fazla içerik dağıtım ağı kullanılacak:** Erişilebilirlik ve yüksek performans için CDN hizmetlerinin kullanımı yaygınlaşacak.
- **Makine öğrenimi yaygınlaşmaya devam edecek:** IDC verilerine göre, 2021 yılında kurumsal ticari uygulamaların yüzde 75'inin arkasında yüksek performans ihtiyacı duyan makine öğrenimi yer alacak.





Türkiye'de İnternet Dolandırıcılığının **Maliyeti %47 Arttı**

Avrupa, Ortadoğu ve Afrika'daki 600'e yakın üst düzey yöneticinin katılımıyla gerçekleştirilen Forrester araştırmasına göre, Türkiye'deki şirketlerin yaklaşık yüzde 60'ı, dolandırıcılık işlemlerinde son 12 ayda artış olduğunu belirtti. İnternet üzerinden gerçekleştirilen dolandırıcılık maliyetinin de son 12 ayda yüzde 47 artışla yükseliş kaydettiği bu dönemde, Türkiye'de dolandırıcılıkla mücadelenin giderek zorlaştığı görülüyor.

Forrester Consulting'in Experian için gerçekleştirdiği araştırmaya göre, Türkiye'deki şirket yöneticilerinin yüzde 90'ı, müşteri deneyiminin iyileştirilmesine öncelik veriyor. Bu oran, EMEA bölgesi ülkeleriyle aynı seviyelerde bulunuyor. Yüzde 87'lik bir kesim ise, gelecek 12 ayda ürün ve hizmetlerini rakiplerden farklılaştırmak istediklerini belirtiyor. Türk şirketlerinin yüzde 87'si, 2018'de coğrafi olarak büyümeye öncelik vermeyi hedeflerken, yüzde 57'si müşteri hizmet maliyetlerinde, yüzde 60'ı müşteri kaybında ve yüzde 50'si ise tahsilat maliyetlerinde son 12 ayda artış olduğunu belirtti.

Experian Türkiye Genel Müdürü Mehmet Bozacıoğlu, Türk şirketlerinin sadece yüzde 17'sinin dolandırıcılıkla mücadelede kullandıkları veri kaynaklarının güncel olduğunu, buna karşılık bu oranın Avrupa'nın diğer ülkelerinde yüzde 31 olduğunu belirtti ve sözlerine devam etti; "Türk şirketlerinin yüzde 50'ye yakın kısmı, tüm müşteri işlemlerinde gerçek zamanlı bir görünürlüğe sahip olduklarını belirtirken, bu oran EMEA bölgesinin diğer ülkelerinde yüzde 33 civarında. Türkiye'deki şirketlerin yaklaşık üçte ikisi, dolandırıcılık işlemlerinde son 1 yılda artış olduğunu belirtirken, internet üzerinden yapılan dolandırıcılığın maliyeti de yüzde 47 artışla son 12 ay içinde yükseliş kaydetti. Türk şirketleri, dolandırıcılığı önleme amaçlı yapılan kontrollerde müşterilerinin bu durumdan etkilenmemesini istiyorlar. Bu doğrultuda, yaklaşık yüzde 60'lık kısım, gelecek 1 yıl boyunca daha fazla pasif kimlik doğrulama yöntemleri uygulamayı planladıklarını belirtiyor."

Şirketlerin ticari önceliklerini gerçekleştirmedeki en büyük engelin dolandırıcılık olduğunu belirten Bozacıoğlu sözlerini sürdürdü, "EMEA bölgesindeki diğer ülkelere paralel olarak, Türk şirketlerinin sadece yüzde 27'si dolandırıcılığın şirket genelindeki etkilerini tam olarak anladıklarını belirtirken, üçte birinden azı, dolandırıcılığın karmaşık yapısıyla kolaylıkla baş edebildiklerini söylüyor. Bu oran Avrupa'nın diğer ülkeleriyle büyük ölçüde aynı seviyelerde seyrediyor. Türk şirketlerinin yüzde 90'ı dolandırıcılığın ne zaman gerçekleşeceğinin daha doğru tahmin edilmesini sağlayan önlemlere yöneldiklerini belirtiyorlar. Bu oran EMEA bölgesinin diğer ülkelerinde ise yüzde 73 seviyelerinde seyrediyor."

Türkiye'de karar alma yetkisine sahip yöneticiler, hızla gelişen dijital ekonomiye ayak uydurmanın önemini anlamış durumdalar. Ancak Türkiye'de şirketlerin sadece yüzde 43'ü veri ve analitik yöntemleri kullanma konusunda, yüzde 47'si ise yasalara uyum süreçlerinde vizyonlarını hayata geçirmekte güçlük çekiyor. Ayrıca Türkiye'deki şirketlerin çoğunluğu (%90) ileri düzey analitik yetkinliklere sahip olmanın kritik bir öncelik olduğunu belirtiyor. Bu şirketlerin yüzde 93'ü, gelecek 12 ay içinde büyük veri teknolojilerine yatırım yapmayı planlıyor. Ancak bugün bile, şirketlerin karar alma yetkisine sahip yöneticilerinin yüzde 48'i hala gerçek verilere güvenmekten çok 'içgüdülerine' veya 'kanaatlerine' güvendiklerini ifade ediyorlar.

Türkiye'deki üst düzey yöneticilerin yüzde 83'ü, gelecek 12 ay içinde müşteri kazanmaya yönelik karar alma süreçlerinde otomasyondan yararlanmayı planlıyor. Bu yöneticilerin yüzde 60'ı, aynı zamanda yüksek riskli alacakların yönetiminde de otomasyondan faydalanmayı planlıyor.





KASPERSKY lab

Fidye Saldırılarının Yüzde 26'sı **Şirketleri Hedef Alıyor**

2017'de fidye saldırılarına maruz kalanların %26,2'sini şirketler oluşturdu. 2016'da bu oran %22,6'ydı. Kaspersky Lab'e göre bunun nedeni, kurumsal ağları hedef alan benzersiz saldırılarla birlikte, şiddeti sürekli artan bu tehdit alanının tamamen değişime uğraması.

2017, fidye yazılımlarının tüm dünyada şirketleri bir dizi solucan tabanlı saldırılarla hedef alarak, ani ve dikkat çekici şekilde geliştikleri bir yıl olarak hatırlanacak. Gerçek amaçları hala gizemini koruyan bu saldırılar arasında 12 Mayıs'taki WannaCry, 27 Haziran'daki ExPetr ve Ekim sonunda gerçekleşen BadRabbit yer alıyor. Bunların her biri kurumsal ağlara sızmak için tasarlanmış saldırılardı. Şirketler ayrıca diğer fidye yazılım çeşitlerinin de hedefi oldular ve toplamda 240.000 kurumsal kullanıcı fidye yazılımlarına karşı koruma altına alındı.

Kaspersky Lab Zararlı Yazılım Kıdemli Analisti Fedor Sinitsyn konuyla ilgili yaptığı açıklamalarda, "2017'nin önde gelen saldırıları suçluların kurumsal hedeflere gösterdikleri ilgiyi ortaya çıkardı. 2016'da tespit ettiğimiz bu eğilim 2017 boyunca hızlandı ve yavaşlama belirtisi de göstermiyor. Şirketler, bireylere kıyasla çok daha yüksek fidye taleplerine maruz kalabiliyorlar ve işlerini sürdürmek için bu fidyeleri ödemeye razı oluyorlar. Uzak masaüstü sistemleri gibi şirket odaklı saldırı yöntemlerinin de artışta olması sürpriz değil" dedi.

2017'deki Diğer Fidye Yazılım Eğilimleri

- 2017'de toplamda yaklaşık 950.000 tekil kullanıcı saldırıya uğradı. Bu sayı 2016'da 1,5 milyondu. Aradaki fark, tespit metotlarının değişmesinden kaynaklanıyor (örneğin: kripto zararlı yazılımlarla sıkça ilişkilendirilen dosya indirme yazılımları artık bulgusal teknolojiler tarafından daha iyi tespit ediliyor. Bu yüzden uzaktan ölçümlerimizin topladığı fidye yazılımlarla ilgili kanılarla birlikte sınıflandırılmıyor).
- Üç büyük saldırı ve AES-NI ve Uiwix gibi daha az bilinen ailelerde, Shadow Brokers'ın 2017 ilkbaharında sızdırdığı açıklar kullanıldı.
- Yeni fidye yazılımı ailelerinin sayısında gözle görülür bir azalma var: 2016'da 62 olan sayı 2017'de 38'e düştü. Öte yandan mevcut fidye yazılımlarına yapılan yeni modlarda artış yaşandı (2016'da 54.000 yeni mod tespit edilirken 2017'de 96.000'den fazlası bulundu). Modlardaki artış, güvenlik çözümleri daha iyi hale geldikçe saldırganların fidye yazılımlarını gizlemeye yönelik ihtiyaçlarını yansıtıyor.
- 2017'nin ikinci çeyreğinden itibaren birçok grup fidye yazılım aktivitelerini sonlandırdı ve dosyaların şifrelerini kaldıran anahtarları yayımladı. Bunlar arasında AES-NI, xdata, Petya/Mischa/GoldenEye ve Crysis bulunuyor. Crysis daha sonra farklı bir grup tarafından yeniden canlandırıldı.
- Şirketlere uzak masaüstü sistemleriyle sızma eğilimi, Crysis, Purgen/GlobeImposter ve Cryakl gibi yaygın ailelerde temel yayılma yöntemi olarak kullanıldığı için 2017'de de büyümeye devam etti.
- Fidye yazılım saldırısına maruz kalan şirketlerin %65'i verilerinin önemli bir bölümünü veya tamamını kaybettiklerini belirttiler. Ödeme yapan şirketlerin altıda biri ise verilerini geri alamadılar. Bu sayılar 2016 verileriyle de tutarlılık gösteriyor.

Öte yandan, Haziran 2016'da başlayan "No More Ransom" girişimi gelişmeye devam ediyor. Hukuk kurumlarıyla güvenlik çözümü geliştiricilerini bir araya getiren bu proje ile büyük fidye yazılımı aileleri takip ediliyor ve faaliyetleri engelleniyor. Böylece bireylerin verilerini geri alması sağlanırken, suçluların iş modeline de zarar veriliyor.

Veeam

Bitcoin Değer Kazandıkça, Kesintiler Daha Çok Can Yakıyor



Ozan İnan
Veeam Türkiye Ülke Müdürü

Sanal para birimi Bitcoin, Chicago'daki CBOE borsasında işlem görmesi ve New York'taki Nasdaq'ın yakında bitcoin işlemlerine başlayacağını açıklamasının ardından değeri hızla arttı. Bu da beraberinde kesintisiz çalışma ve erişilebilirlik sorularını getirdi. Her ne kadar Deutsche Bank, 2018'in en büyük riski olarak Bitcoin'deki çöküşü görse de, bitcoin bundan etkilenmeyerek değer kazanmaya devam ediyor.

Bitcoin'in hızla değer kazanması, paranın tüm yıl boyunca kesintisiz olarak alım satımının yapılmasını hiç olmadığı kadar önemli hale getirdi. Geçen hafta sonu ABD'nin en büyük Bitcoin işlemci şirketlerinden biri olan Gemini'nin yaşadığı kesinti de gösteriyor ki para değişimi yapan kullanıcılar için bir dakikalık kesinti bile işlerine muazzam derecede etki edebiliyor ve kaçırılan fırsatlar kar ve zarar etme arasındaki farka sebep olabiliyor.

Planlı kesinti, hizmet aksamasında bir defaya mahsus kabul edilebilir bir özür gibi düşünülse de, dijitali bilen modern müşteriler, dijital hizmetlere kesintisizce ulaşabilmeyi artık mutlak bir gereksinim olarak görüyor. Gemini'daki kesintiyi bir müşteri sosyal medya şöyle değerlendirdi: "Mevzuatla uyumluluk için sistemlerinizde bakım yapıyorsunuz. Ama sonuç olarak ben kaybediyorum."

Ayrıca, bu tür bir kesintinin şirket üzerinde yarattığı sonuçlar gerek finansal gerekse itibar olarak da çok olumsuz. Şirketlerin kesintisiz çalışabilmesine yönelik çözümlerin yenilikçi tedarikçisi Veeam® Software'in yılın ilk aylarında gerçekleştirdiği araştırmaya göre bir kesinti İngiltere'deki işletmelere yılda ortalama 17,9 milyon sterline mal oluyor. Dahası, erişilebilirlik konusunda problem yaşanması marka itibarını zedeliyor ve müşteriler işlerini rakip firmalara götürüyorlar. Günümüzün teknolojiyi iyi bilen kullanıcıları hiç olmadığı kadar zor affediyor ve milyarderler tarafından desteklenen işletme fonları bile bu kesintilerin getireceği müşteri kaybını göze alamıyor.

Son gelişmeleri değerlendiren Veeam Türkiye Ülke Müdürü Ozan İnan, Bitcoin sağlayıcılarının artık erişilebilirliğin yeni bir tanımı üzerinde kafa yorduğunu belirtiyor. İnan sözlerine şöyle devam ediyor. "Bu yeni tanımda 'planlı kesintiler' yok, veri ve hizmetler her an erişilebilir olmak zorunda. İşletmeler iş avantajı yaratmak için tam da bu yüzden yedeklemelerini kullanıyorlar. En güncel yedeklenmiş verilerini kullanarak sitelerinin simülasyonu üzerinde ihtiyaç duyulan bakımı gerçekleştirebiliyor ve kesintisiz hizmeti garantiliyorlar. Bunun sonucunda da müşteriler, uluslararası Bitcoin Exchange ofisinden de bahsediyor olsak, yerel bir işletmeden de bahsediyor olsak güvenle hizmet almaya devam edebiliyor."

Veeam® Software Hakkında:

Veeam dünya çapında kesintisiz çalışmayı gerçekleştirme sırasında şirketlerin karşılaştığı zorlukların farkında. İşletmeler tüm yıl boyunca 7/24 çalışmak zorunda. Veeam şirketlerin kesintisiz çalışması adına yeni bir pazara öncülük ederek şirketlerin kurtarma zamanı ve nokta hedeflerini (RTPO) tüm uygulamalar ve veriler için 15 dakika ya da daha azında gerçekleştirmelerine yardımcı oluyor. Bu talebi karşılamak amacıyla yüksek hızlı kurtarma, veri kaybının önüne geçme, kanıtlanmış koruma, yedeklenen veriden faydalanma ve uçtan uca görüntüleme sağlıyor. Veeam Backup & Replication™'ı içeren Veeam Availability Suite™, işletmelerin zaman kazanması, riskleri azaltması ve sermayeyle operasyonel harcamaları gözle görülür şekilde düşürmesine yardımcı olacak modern veri merkezinin sanallaştırma, depolama ve bulut teknolojilerini bir üst seviyeye taşırken Veeam müşterilerinin bugünkü ve gelecekteki iş hedeflerini de destekliyor.

2006'da kurulan Veeam'in 51.000'den fazla ProPartner'ı ve dünya çapında 267.500'ün üzerinde müşterisiyle sektördeki en yüksek müşteri memnuniyeti değerlerine sahip. Merkezi İsviçre'nin Baar şehrinde bulunan ve 30'dan fazla ülkede ofisi bulunan Veeam hakkında daha fazla bilgi için http://www.veeam.com'u ziyaret edebilir ya da Twitter'da @veeam hesabını takip edebilirsiniz.

VEEAM

Siber Ataklara, Fidye yazılımlarına, Güvenlik Açıklarına Karşı Sigorta Poliçeniz Veeam.

İş Sürekliliği için Veeam Availability Platformuna Geçin.



www.veeam.com/tr

#1 AVAILABILITY
Any app · Any data · Any cloud

TechData

Tech Data FutureIT Etkinliği Sektörü Buluşturdu

"Teknolojinin Gücüyle Dünyaya Bağlanın" temasıyla hazırlanan Tech Data FutureIT, BT sektörünün yeni ihtiyaçlara göre şekillenen yapısını, küresel bazda önde gelen teknoloji şirketlerinin penceresinden görebilme imkânını sundu.



Tech Data Türkiye tarafından 6 Aralık 2017 tarihinde ikinci kez düzenlenen Tech Data FutureIT etkinliği, BT sektörünün karar vericilerini ve kanal iş ortaklarını Hilton İstanbul Bomonti Otel'de buluşturdu. Açılış konuşmasını yapan Tech Data Türkiye Genel Müdürü Hakkı Eren, geçen yıl gerçekleştirilen ilk toplantıdaki 'Avnet' kimliğinin artık 'Tech Data' olduğuna dikkat çekerek, şu bilgileri verdi:

"Tech Data Türkiye'nin iki ortağı var: Biri Tech Data Global, ikincisi ise Sanko Holding. Tech Data; dünyanın en büyük küresel BT distribütörlerinden biri olarak, veri merkezinden oturma odamıza kadar tüm BT ürün ve çözümlerinin satışı, kurulumu ve katma değerli hizmetler ekleyerek sunma yetkinliklerine sahip bir yapı. FutureIT toplantısında amacımız; Türkiye BT ekosistemine dünyanın dev teknoloji üreticilerinin vizyonlarını bir arada bulabilecekleri, teknolojinin geleceğini ilk ağızdan, bunu üreten firmaların en üst düzey yöneticilerinden öğrenme imkânı sunmak. Bilgi teknolojilerinde değişimde odak noktamız 'veri' ve artan veri etrafında şekillenen verilerin depolanması, korunması ve işlenmesi, değerlendirilmesi ve bu verilerle kararlar verilmesi süreçleri. Çünkü alınacak kararlar, şirketlerin başarılarını etkileyen temel konu olacak. Doğru bilgiyi işleyerek, doğru kararları vermeye destek sunmak önem taşıyor. Biz Tech Data olarak BT sektöründe vizyon ve kabiliyetlerimizle işletmeleri ve iş ortaklarımızı geleceğe taşımaya hazırız."

Farkındalık Tamam Ama Plan Yok

Hakkı Eren'in ardından sözü alan Dell EMC Ülke Müdürü Sinan Dumlu da, Dell ve EMC entegrasyon süreci hakkında detayları paylaştı. Resmi birleşme sonrası, yılı 76 milyar doların üzerinde kapatacaklarına yönelik beklentilerini dile getiren Dumlu, dönüşümün artık yüksek Ar-Ge bütçelerini gerekli kıldığına işaret etti. "Ar-Ge'ye 4,5 milyar dolar para harcamayı taahhüt ettik ve 20 binin üzerinde patent veya patent başvurumuz var" diyen Sinan Dumlu, birleşme sonrası Türkiye pazarındaki durumu ise şöyle anlattı: "Birleştikten sonra iki çeyrek içinde PC pazar payımız yüzde 5 arttı. Sunucu pazar payı da yükselirken, depolamada flash ile sektör lideriyiz. Türkiye'de iyi bir entegrasyon yaptık. İddialı olduğumuz üç başlık var: İyi tarif ediyoruz, ne yapacağınızı net söylüyoruz ve son olarak, bunu yapmak istediğinizde gereken ürün ve çözümleri size verebiliyoruz. Dijital transformasyonun alt başlıkları büyük veri ve analizi, Endüstri 4.0, IoT. Türkiye'de bu konuda farkındalık yüksek, ama bunu destekleyecek plan yok. Biz dijital transformasyon konusunda danışmanlık hizmetlerimizle yardımcı olmaya hazırız."

Uçtan uca çözüm ve entegrasyon içinde bulunduğumuz süreci 'dijital bir girdaba' benzeten Cisco Türkiye İş Ortakları Organizasyon Lideri Emre Yükselci, hayatımızın ve iş yapış şekillerimizin de değiştiğini vurguladı. Dijital girdapla birlikte şirketler değişiyor ve dijital ekonomiye değer getirecek dijital fırsatlara sahip endüstriler var. "Cisco ve iş ortaklarımızla yaptığımız proje ve uygulamalarla müşterilerin hayatına dokunduğumuz çözümler sunuyoruz" diyen Emre Yükselci, şöyle devam etti: "Yeni nesil network ve sezgisel ağ dediğimiz bir kavram duyurduk. Kendi kendine öğrenen ve tehditlere karşı sizi sürekli koruyan bu altyapı ve ağ yapısı. Geleceğin "network"ünün böyle oluşacağını öngörüyoruz. Uygulamaların sağlıklı çalışması önemli ve Cisco bu konuda da çözümler sunuyor. Güvenlik tarafında ise saldırganlar sofistike hale gelirken, koruyanlar da daha bilgili hale gelmeli. Bu çözümlerin birbiri ile haberleşmesi de önemli. Biz bunları adreslemek adına uçtan uca çözümlere ve entegrasyona odaklanıyoruz. 2018 başında inovasyon merkezimiz de açılacak."


Hakkı Eren

Tech Data
Advanced Solutions

SANKO

FutureIT

Teşekkürler

6 Aralık 2017 tarihinde gerçekleştirdiğimiz FutureIT konferansımıza katılım ve sunumlarıyla katkıda bulunan lider teknoloji üreticilerine teşekkür ederiz.































Yaklaşan Tehlike Siber Zorbalık

Teknolojinin gelişimi ile birlikte hızla yayılmaya başlayan siber zorbalık, dünya nüfusunun yüzde 15'ini tehdit eder boyutlara ulaştı. Yapılan araştırmalara göre siber zorbalığı yapanlar ağırlıklı olarak erkeklerden oluşurken, bu tür zorbalığa maruz kalanlar ise genellikle kadınlar oluyor.

Yeşilay ve KÜLT Vakfı iş birliğiyle düzenlenen 4. Uluslararası Teknoloji Bağımlılığı Kongresi'nin ikinci gününde dünyada yayılmaya başlayan siber zorbalık konusu da ele alındı. Yeşilay Genel Başkan Yardımcısı Dr. Mehmet Dinç, Türkiye'de henüz pek fazla görülmese de, yaklaşan bir tehlike olarak, siber zorbalık konusunda farkındalık oluşturulması gerektiğinin altını çizdi. Teknolojinin gelişimi ile birlikte hızla yayılmaya başlayan siber zorbalık, dünya nüfusunun yüzde 15'ini tehdit eder boyutlara ulaşmış durumda. Yapılan araştırmalara göre siber zorbalığı yapanlar ağırlıklı olarak erkekler olurken, bu tür zorbalığa maruz kalanlar ise genellikle kadınlar oluyor.

Kongrenin "Siber Zorbalık" başlıklı oturumuna moderatörlük yapan Yeşilay Genel Başkan Yardımcısı Dr. Mehmet Dinç, siber zorbalığın geleneksel zorbalıktan en büyük farkının sayısız olması olduğunu kaydetti. Geleneksel zorbalığa insanların sayılı kez maruz kalabileceklerini ifade eden Mehmet Dinç, "Bu sayı 3-5 ya da en fazla 10 olur. Ama siber zorbalığın sayısı yok. Gece gündüz, sabah akşam her an defalarca buna maruz kalabilirsiniz. Bir kitlesi de olmayan siber zorbalığın etkisi ve zararı oldukça fazla. Aylarca devam eder ve kaçılamaz bir durumdur. Bu sebeple dünyada canına kıyan insanları bile görmeye başladık" dedi. Türkiye'de henüz pek fazla görülmese de, yaklaşan bir tehlike olarak, bu konuda farkındalık oluşturulmasında fayda olduğunu söyleyen Mehmet Dinç, siber zorbalığı daha iyi tanımlayan araştırmalar ve bu konuda bilinçlendirmeyi artırıcı çalışmaların yapılması gerektiğini bildirdi.

Oturumda "Türkiye'de Siber Zorbalık Çalışmalarının Durumu" başlıklı bir sunum gerçekleştiren Yeşilay Bilim Kurulu Üyesi Prof. Dr. Osman Tolga Arıcak ise, çocukları siber zorbalık yapan ya da buna maruz kalan ailelerin, bu konuda ne yapacaklarını bilmediklerini belirtti. Ailelerin siber zorbalık ile ilgili bilgi ve birikiminin geliştirilmesi gerektiğinin altını çizen Arıcak, "Aile ve okulların yanı sıra Milli Eğitim Bakanlığı, İçişleri Bakanlığı, Gençlik ve Spor Bakanlığı, Aile ve Sosyal Politikalar Bakanlığı, yerel yönetimler ve medyanın bu mücadeleye destek vermesi gerekiyor" dedi.

Dr. Zsolt Demetrovics ise "Siber zorbalık" başlıklı sunumunda geleneksel zorbalık ile siber zorbalığı karşılaştırdı. Geleneksel zorbalığı agresif, fiziksel ve sözsel eylemlerin güç denemesi olarak birleştirilmesi şeklinde tanımlayan Dr. Zsolt Demetrovics, "Tekmelemek, tehdit etmek geleneksel zorbalığın belirtileridir. Geleneksel zorbalığa dünya nüfusunun 3'te biri maruz kalıyor" dedi. Siber zorbalığın ise elektronik ortamda yapıldığını vurgulayan Dr. Zsolt Demetrovics, "Rahatsız eden mesajlar ya da fotoğrafların paylaşılması, biri hakkında dedikodunun yayılması gibi konular siber zorbalık alanına giriyor. Dünyada siber zorbalığa maruz kalanların oranı yüzde 15" dedi. Siber zorbalığın görülme sıklığının henüz geleneksel zorbalık kadar yüksek olmadığına da dikkat çeken Dr. Zsolt Demetrovics, "Geleneksel zorbalığa erkekler, siber zorbalığa ise daha çok kadınlar maruz kalıyor. Her iki zorbalık türünde de zorbalar daha önce mağdur olan insanlardan oluyor" dedi.







3. Uluslararası Siber Savaş ve Güvenlik Konferansı Gerçekleştirildi

Bu yıl 3'üncüsü düzenlenen Uluslararası Siber Savaş ve Güvenlik Konferansı (International Cyber Warfare and Security Conference), 27-28 Kasım 2017 tarihlerinde Ankara'da; Savunma Sanayii Müsteşarlığı tarafından, Başbakanlık, Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilim Sanayi ve Teknoloji Bakanlığı, Kalkınma Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, TÜBİTAK ve SASAD'ın destekleri ve Defence Turkey dergisi organizasyonu ile gerçekleştirildi.

Etkinlik, Bilgi Teknolojileri Kurumu Başkan Yardımcısı Dr. Ahmet Kılıç, Savunma Sanayii Müsteşar Yardımcısı Mustafa Şeker ve NATO Altyapı Hizmetleri Direktörü Dr. Gregory B. Edwards'ın yaptıkları açılış konuşmaları ile başladı. Oturumlar, farklı ülkelerden siber güvenlik yöneticileri, uzmanları, NATO ve Türk temsilcilerinin panel oturumları ile devam etti.

Konferansın ana teması bu yıl "Siber Güvenlik Ekosisteminin Geliştirilmesi ve Kümelenme" olarak belirlendi ve bu kapsamda konferans öncesinde gerçekleştirilen Akademi, Kamu ve Özel Sektör Çalıştayları sonucunda ortaya çıkan ülkemizde Siber Güvenlik Kümelenmesi kurulmasına yönelik model çalışmaları, etkinliğin 2. gününde Savunma Sanayii Müsteşarlığı (SSM) Siber Güvenlik ve Elektronik Harp Sistemleri Daire Başkanı Muhammet Sami Ulukavak'ın açılış konuşmasında katılımcılarla paylaşıldı.

3. Uluslararası Siber Savaş ve Güvenlik Konferansı'nın sonunda, siber güvenlik kümelenmesi kapsamında insan kaynağı eksikliğinin giderilmesine yönelik siber güvenlik akademisi çalışma grubunun oluşturulması için Savunma Sanayii Müsteşarlığı ile Ortadoğu Teknik Üniversitesi (ODTÜ) ve İstanbul Üniversitesi (İTÜ) arasında iyi niyet anlaşması imzalandı.

İmza töreninin ardından Savunma Sanayii Müsteşar Yardımcısı Mustafa Şeker tarafından ülkemizde siber güvenlik alanında siber güvenlik kümelenmesi kurulacağı ve buna yönelik çalışmalara başlanıldığı duyuruldu.





SHIELD 2017 Konferansı Gerçekleştirildi

Türkiye'nin lider güvenlik entegrasyonu ve danışmanlığı şirketlerinden biri olan Innovera tarafından bu yıl 3. kez düzenlenen SHIELD Güvenlik Konferansı, dünyaca ünlü güvenlik uzmanı Edward Snowden'ın güvenlik sektörüne yönelik merak edilen soruları yanıtlamasıyla başladı.

Siber güvenlik alanında sağladığı öncü danışmanlık, teknoloji ve saha hizmetleri ile tanınan Innovera, SHIELD Siber Güvenlik Konferansı, "Dijital Geleceği Güven Altına Almak" teması ile 21 Kasım 2017 tarihinde, İstanbul Çırağan Palace Kempinski'de gerçekleşti. Okan Bayülgen ve Burcu Bakdur'un sunuculuğunu üstlendiği konferansta, siber güvenlik sektörünün çehresini değiştirecek yenilikler ve çözümler konuşuldu. Sabahın erken saatlerinde büyük bir ilgiyle başlayan siber güvenlik konferansı SHIELD 2017, ulusal ve uluslararası çapta önemli konuşmacıları, bine yakın üst düzey yönetici ve güvenlik uzmanını ağırladı.

"Dijital Geleceği Güven Altına Almak"

"Dijital Geleceği Güven Altına Almak" temasıyla siber güvenliğin dijital dönüşümde kilit rol oynayacağını belirttiği açılış konuşmasında Innovera Genel Müdürü Gökhan Say, "Bu sene Innovera olarak 10.cu yılımızı kutluyoruz. Aynı zamanda Bilişim 500 listesinde tüm güvenlik entegratörleri arasında birinci olmanın mutluluğunu yaşıyor, bu kapsamda yatırımlarımıza da hız kesmeden devam ediyoruz. İki sene önce Innovera ekibi olarak 40 kişiyken bugün 120 kişiyiz. 2020 yılında ise 250 kişi olmayı hedefliyoruz. İki yıl önce Innovera çatısı altında başlattığımız Ar-Ge ürünümüz Atar, Diffusion Capital Partners'dan (DCP) aldığı çekirdek yatırım ve güçlü yönetim kadrosuyla bugün Atar Labs olarak Orta Doğu ve Avrupa'da bir çok ülkede faaliyet göstermeye başladı. Bu çalışmalarımızla global arenada Türkiye'yi temsil etmiş olmanın heyecanını yaşıyoruz. Son 20 yıl içerisinde zararlı kod sayısı yıllık 5.000'den 600 milyona çıkmış durumda. IoT, yapay zekâ, robotların hayatımıza hızla girmesiyle beraber tehditlerde artışın daha da hızlanacağını görüyoruz. Siber güvenlikte pek çok bilinen ve bilinmeyen



konular üzerine kurguladığımız bu seneki SHIELD 2017 konferansının, tüm sorunlarına çözüm bulan bir platform olmasını diliyorum" dedi.

Siber Güvenlik Tüm Dünya İçin Önemli Bir Gündem Maddesi

Siber saldırılar ve dolayısıyla veri güvenliğinin, bugün kurumların ötesinde tüm dünya ülkeleri için önemli bir gündem maddesi olduğunu belirten DenizBank Genel Müdürü Hakan Ateş, finans teknolojilerinin ötesinde, siber güvenlik de dâhil olmak üzere tüm teknolojik gelişmeleri yakından takip ettiklerini söyledi.

Büyük hızla ilerleyen dijitalleşme çağında kurumların ve resmi otoritelerin hep beraber oluşturacakları ekosistem içerisinde iş birliği ile hareket edilmesi gerektiğinin altını çizen Ateş, şöyle konuştu: "Bugüne kadar, inovasyon üssü olarak tanımladığımız teknoloji iştirakimiz InterTech'in öncülüğünde, finans sektörüne teknoloji alanında pek çok inovatif ürün ve uygulamayı kazandırdık. Dijitalleşmenin hayatımıza her gün daha fazla nüfuz ettiği günümüzde bilgi güvenliği de artarak önem kazanıyor. Yaşanan süreç, bir ekosistem ihtiyacı ve bu ekosistem aslında rakip gibi görünen yeni partnerlerinizi ortaya çıkarıyor. Biz de hem rekabetin hem de işbirliğinin bir arada olduğu 'Rekabetlik' ifadesi ile tanımlayabileceğimiz bir anlayışa evriliyoruz. Dolayısıyla zamanında Wells Fargo'nun CEO'su John Gerard Stumpf'ın işaret ettiği, "bankaların öğle yemeğini yiyen" finansal teknoloji şirketlerini (FinTech) rakip değil, bir arada sonuç üreteceğimiz yapılar olarak görüyoruz."

"İnternette Yaşıyorum, Rusya'da Uyuyorum"

Dijital dünyada edindiği güvenlik ve gizlilik alanındaki tecrübelerini paylaşan ABD'li siber güvenlik ve bilgisayar uzmanı olan Edward Snowden, ilk kez Türkiye'de sektör uzmanlarıyla bir araya geldi. "Yeni Jenerasyon Mahremiyet & Güvenlik İkilemi Nasıl Çözülecek?" başlıklı konuşması ile Snowden, dijitalleşme ile birlikte büyük bir önem kazanan mahremiyet ve güvenlik konularına ışık tuttuğu konuşmasında şunları dile getirdi: "Güvenlik problemlerinin her geçen gün arttığı karanlık bir dönemdeyiz. Bize sunulan dünyayı olduğu gibi kabul etmek zorunda değiliz. Dünyayı değiştirmek ve daha iyi bir yer haline getirmek için çalışmalıyız."

Shield 2017 Siber Güvenlik Konferansı, "Dijital İnovasyon ile Gelen Güvenlik Riskleri: Güvenli Bir Dijital Gelecek İçin Stratejimiz Ne Olmalı" ve "Hayal mi Yoksa Gerçek mi? Siber Güvenlikte Yeni Nesil Otomasyon ve Geleceği" panelleriyle devam etti. Panellerde, dijital güvenlik riskleri ve çözüm stratejileri ele alındı.





Türkiye'nin bilişim altyapısının öncüsü Netaş, 50. kuruluş yıdönümünü Ankara'da düzenlediği etkinlikle kutladı. Türkiye Cumhuriyeti Başbakanı Binali Yıldırım'ın konuşma yaptığı toplantıda Netaş ve yeni hissedarı ZTE, Türkiye'de gerçekleştirecekleri yeni yatırımların imzasını attı. Netaş ve ZTE Corporation, üç farklı yatırıma ilişkin mutabakat anlaşmasına imza attı.

NETAŞ ve ZTE'den Türkiye'de Ar-Ge Atağı

Türkiye'yi Bilişim Teknolojileri Merkezi Yapacak Üç Yatırım

Anlaşma uyarınca, Netaş ve ZTE, 2018 yılında, demir yollarına özel kablosuz geniş-bant iletişim standardı olan GSM-R alanında ortak Ar-Ge çalışması yürütecekleri bir GSM-R Mükemmeliyet Merkezi açacak.

Bunun yanı sıra Netaş, Avrupa, Orta Doğu ve Afrika bölgelerinde ZTE ürünleri için tamir, bakım ve destek hizmetleri sağlayacak. Bu iş birliğinin ZTE ürünlerinin, dolayısıyla Netaş'ın pazarını genişletirken, müşteri memnuniyetini artırması, diğer taraftan Netaş'ın gelirlerini büyütürken Türkiye'nin hizmet ihracatına da katkıda bulunması bekleniyor.

Son olarak, ZTE'nin Avrupa, Orta Doğu, Afrika ve Orta Asya bölgelerindeki müşteri ve çalışanlarına yönelik gerçekleştirilecek eğitim hizmetleri "Netaş Akademi" üzerinden sağlanacak. Akademi, Türkiye'de bilişim profesyonellerinin yetişmesinde rol oynarken, diğer taraftan Türkiye'nin yüksek katma değerli hizmet ihracatını destekleyeceği düşünülüyor.

Etkinliğe Başbakan Binali Yıldırım da Katıldı

Netaş'ın 50. kuruluş yıldönümü etkinliğinde konuşma yapan Türkiye Cumhuriyeti Başbakanı Binali Yıldırım ise şöyle konuştu: "Birinci önceliğimiz, yerli teknolojiye sahip katma değeri yüksek ürünler geliştirmek, işte Netaş ve ZTE birlikteliğinin de önemi burada ortaya çıkıyor. Çin'in önemli bilgi iletişim firması son 10 yıldır Türkiye'de bulunuyor, Türklerle tanıştı ve bu aşamada da Türkiye'nin bilgi iletişim, Ar-Ge konusunda en önemli firmalarından biri olan Netaş'la bir birlikteliğe gitti ve gücüne güç kattı. Bundan sonra yapacağınız iş, burada Türk mühendisinin akıl teriyle, Türk işçisinin alın teriyle yerli içeriği daha fazla ürünler yapmak ve bu ürünleri Türkiye'nin dâhil olduğu ve 4 saat uçuşla 56 ülkeye, 1,5 milyar nüfusa ulaşacak, yıllık 31 trilyon dolar bir varlığın, gelirin, gayrisafi hasılanın olduğu bu alanda en güzel şekilde değerlendi-



receksiniz. Yeni Türkiye sadece iç pazarla ekmek yediğiniz bir yer değil, bütün küresel pazara, bölgesel pazara da açılacağınız önemli bir merkez olacaktır. Bundan sonraki hedef bu olmalıdır. Bu konuda da gereken her türlü çalışmanın yapılacağından zerre kadar şüphem yoktur. Biz bu konuda hükümet olarak bugüne kadar Netaş'a ne destek verdiysek, bugün ZTE-Netaş birlikteliğine de aynı desteği vermeye devam edeceğiz," dedi.

"Milli ve Yerli 5G Konusunda Netaş ve ZTE'den Çok Şey Bekliyoruz"

Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan da katıldığı etkinlikte konuşma yaptı. Ahmet Arslan, teknoloji üreten toplum hayalinde önemli görevler üstlenen, bilgi ve telekomünikasyon sektörüne yön veren Netaş'ın bu yolda yarım asrı geride bırakmasının gururunu yaşadıklarını belirtti.

Arslan konuşmasına şöyle devam etti: "Türkiye'nin bilişim dünyasında yerini alması, hatta öncü ülkeler liginde yer alması için 15 yıldır önemli yatırımlar yapıldı. Adeta bilişim ve haberleşme dünyasının üzerine titrendi. Bu noktada milli ve yerli 5G konusunda ZTE'den çok şey bekliyoruz."

Netaş Bilişim Teknolojilerinde Yerliliğin Öncü Firması Olmaya Devam Edecek

Toplantıyı "Netaş'ın kuruluşu, Türkiye'de telekomünikasyon sanayinin de ilk temel taşıdır," diyerek açan Netaş CEO'su C. Müjdat Altay, "Kurulduğumuzdan bu yana ülkemize hep en yeni bilgi ve iletişim teknolojilerini sunan şirket olduk. Bu sayede ülkemize 3 milyar doların üzerinde döviz kazandırmanın gururunu yaşadık." dedi. "Son on yılda 10 kat büyürken, Türkiye'nin ve bölgemizin dijital dönüşümü için telekom, finans, sağlık, enerji, spor, eğitim, kamu ve savunma gibi dikeylerde akıllı çözümler uyguladık. Bugün itibarıyla Türkiye'nin lider sistem entegratörü ve yazılım ihracat şampiyonuyuz" diyen Netaş CEO'su sözlerini şöyle sürdürdü:

"Netaş, 50. yılına dünyanın en büyük bilişim şirketlerinden biri olan ZTE ile girdi. ZTE firmasının bu yatırımı Türkiye'ye teknoloji geliştirme amaçlı yapılmış en büyük yatırımlardan biri. İkinci 50 yılımızda da ZTE ile beraber çok daha güçlü olacağımıza ve teknoloji alanında yeni ufuklar açıp bölgenin yüksek teknoloji merkezi olacağımıza yürekten inanıyoruz. Netaş bilişim teknolojilerinde Türkiye'nin, yerliliğin öncü firması olmaya devam edecek."

Amacımız Netaş'ı EMEA Bölgesinde Teknoloji Üssü Haline Getirmek

Toplantıda konuşan ZTE Corporation Yönetim Kurulu Başkanı Yin Yimin ise, "ZTE'nin Çin dışında tek seferde en büyük yatırımını Netaş ile Türkiye'ye yaptık. Amacımız Netaş ve Türkiye'yi EMEA bölgesinde bir teknoloji üssümüz haline getirmek." ifadelerini kullandı.

ZTE olarak Netaş'ın gelişimi için yatırım yapmaya devam edeceklerini söyleyen Yin, "Türkiye'nin bilişim sektöründe hedeflenen atılımı gerçekleştirilebilmesine yönelik olarak ZTE 4.5G'nin Türkiye'de yerelleştirilmesi için patent, bilgi birikimi, tasarım ve inceleme, tedarik zinciri ve dokümantasyon desteği sağlayacağız." dedi.

Yin, Çin'in Tek Kuşak Tek Yol girişimi ile Türkiye'nin 2023 hedeflerinin paralellik taşıdığını söyleyerek, "Önümüzdeki beş yıl içinde hükümetlerimizin, müşterilerimizin ve yatırımcılarımızın desteği ile Netaş'ın değerini 1 milyar dolara ulaştıracağımıza inanıyoruz." açıklamasını yaptı.

Çok uluslu bilişim çözüm ve sistemleri üreticisi ZTE, Netaş'ın, One Equity Partners'ın yönettiği bir portföy şirketi olan OEP Turkey Tech B.V.'ye ait yüzde 48.04 hissesini geçtiğimiz 28 Temmuz 2017 tarihi itibarıyla satın almıştı.

Netaş 50. Yıl Etkinliğinde Birbirinden Önemli İsimleri Ağırladı

Netaş'ın Ankara'da düzenlediği 50. Yıl Ankara Zirvesine Başbakan Binali Yıldırım'ın yanı sıra, Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanı Ahmet Arslan, Çin Halk Cumhuriyeti Türkiye Büyükelçisi Yu Hongyang, ZTE Kıdemli Yönetim Kurulu Başkan Yardımcısı ve Stratejiden Sorumlu İcra Kurulu Üyesi Jie Chen, Küresel Satıştan Sorumlu Başkan Zhang Zhenhui ve kamu ve özel sektörlerden 1.000'in üzerinde profesyonel katıldı.



Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan

INFRASKOPE



Edward Snowden

AMERİKA'NIN EN SIKI KORUNAN HÜKÜMET BİRİMİ

NSA'den 1.8 milyon gizli doküman çaldı.

GÜVENLİK ALTYAPINIZ BU TÜR OLAYLARI

TESPİT EDEBİLİYOR MU?

karmasis

GÜVENLİK FARKINDALIKLA BAŞLAR ™

FARKINDA OLMADIĞINIZ BİR TEHLİKE İÇİN ÖNLEM ALAMAZSINIZ.
INFRASKOPE KURUMUNUZDA GERÇEKLEŞEN OLAYLARI GÖRMENİZİ
VE ÖNLEM ALMANIZI SAĞLAR.

info@karmasis.com

50 yıl

YENİ NESİL YÖNETİLEN HİZMETLERLE YANINIZDAYIZ.

Netaş Siber Operasyon Merkezi ile kurumların siber güvenlik, ağ ve sistem operasyonları Netaş güvencesinde.

NETAŞ

netas.com.tr

1982'den beri GÜVEN yazıyoruz...

Komuta Kontrol ve Savaş Sistemleri

Eğitim Teknolojileri ve Simülasyon Sistemleri

Yönetim Bilgi Sistemleri

Ülke ve Siber Güvenlik Çözümleri



Akıllı Teknolojiler, Entegre Çözümler



HAVELSAN A.Ş. Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.